

For Reference

NOT TO BE TAKEN FROM THIS ROOM

For Reference

NOT TO BE TAKEN FROM THIS ROOM

Ex LIBRIS
UNIVERSITATIS
ALBERTAENSIS





Digitized by the Internet Archive
in 2018 with funding from
University of Alberta Libraries

<https://archive.org/details/Riddell1960>

Thesis
1961
#39

THE UNIVERSITY OF ALBERTA

ON BASES FOR SETS OF INTEGERS

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE

OF MASTER OF SCIENCE

DEPARTMENT OF MATHEMATICS

by

James Riddell

EDMONTON, ALBERTA

December, 1960

ABSTRACT

This thesis deals with some aspects of additive number theory. The first two chapters are concerned with the representation of integers as sums of a fixed number of integers from a given set. The third chapter deals with the representation of integers as differences between integers from a given set. In the last chapter we consider some results of Erdős, Fuchs, Lorentz, and Turán on related problems.

ACKNOWLEDGEMENTS

The writer would like to thank Dr. Leo Moser for his guidance and advice.

TABLE OF CONTENTS

	Page
INTRODUCTION	i
CHAPTER I. ON h -BASES FOR AN INTEGER n	
1. Introduction	1
2. Upper and lower estimates for $k_2(n)$	4
3. The function $n_h(k)$	19
4. An analogous problem in set theory	34
CHAPTER II. BASES FOR THE INTEGERS	
5. Introduction	37
6. On the ratio $\frac{B(n)}{h\sqrt{n}}$	39
7. A theorem of Cassels	56
CHAPTER III. DIFFERENCE BASES	
8. Introduction	60
9. On the ratio $\frac{k(n)}{\sqrt{n}}$ and $\frac{l(n)}{\sqrt{n}}$	62
CHAPTER IV. SOME RELATED PROBLEMS	
10. Introduction	71
11. Some results of Erdős, Turán, and Fuchs	71
12. A theorem of Lorentz	75
13. B_2 sequences	82
BIBLIOGRAPHY	88

INTRODUCTION

In Chapter I we discuss problems on bases for an integer n , a basis of order h for n being defined as a set of integers whose set of sums h at a time contains the integers $0, 1, 2, \dots, n$. We obtain an improvement on a result of Moser [21], and extend some results of Stöhr [31].

In Chapter II we consider some results of Stöhr [31] and Cassels [3] concerning bases for the entire set of non-negative integers.

In Chapter III we present some results of Rédei and Rényi [25], and some extensions of these obtained by Leech and Hazelgrove [18], [19]. The problems dealt with by Rédei and Rényi concern the representation of each of the integers $1, 2, \dots, n$ as the difference between some two elements of a given set of integers. The given set is called a difference basis for n if all of $1, 2, \dots, n$ can be represented.

In Chapter IV we consider some problems concerning sums of pairs of integers from sequences that are not necessarily bases. We include results of Erdős, Turán, Fuchs [14], [12], and Lorentz [20].

CHAPTER I

ON h-BASES FOR AN INTEGER n

1. Introduction

In this chapter we consider some results of Rohrbach [26], Moser [21], and Stöhr [31] concerning the representation of the integers $0, 1, 2, \dots, n$ as sums of a fixed number of integers from a given set.

Let $h \geq 1$ and $n \geq 0$ be integers. A subset A of the numbers $0, 1, \dots, n$ is called an h -basis for n , or a basis of order h for n , if each of the numbers $0, 1, \dots, n$ is representable as the sum of h numbers from A , repetitions being allowed. By a minimal h -basis for n is meant an h -basis for n with the least possible number of elements. We designate the number of elements in a minimal h -basis for n by $k_h(n)$. Sometimes, when the meaning is clear, we shall say "basis for n " or "basis" instead of " h -basis for n ".

We make some remarks and give some illustrative examples in connection with these definitions. The set $0, 1, h+1, 2h+1, \dots, m h+1$ is an h -basis for $(m+1)h$. For, any n in the interval $1 \leq n \leq (m+1)h$ can be written in the form $(jh+1) + r$, where $0 \leq j \leq m$ and $0 \leq r \leq h-1$; the elements from the given set used to express such an n are $j_{h+1}, 1$, and 0 , with 1 repeated r times and 0 repeated $h-1-r$ times to give the desired h summands. 0 is represented as the sum of h zeros.

The set is not, in general, a minimal h -basis for $(m+1)h$, for let $h = 2$, and let $m \geq 4$, say. Our set becomes $0, 1, 3, 5, 7, 9, \dots, 2m+1$, a 2-basis for $2(m+1)$ with $m+2$ elements. Replacing the two numbers 5 and 7 here by 4 yields a 2-basis for $2(m+1)$ with $m+1$ elements. On the other hand, for the trivial case with $h = 1$, the only (and hence minimal) basis for n is $0, 1, 2, 3, \dots, n$, and $k_1(n) = n+1$. Note that the numbers 0 and 1 are both required in any h -basis for $n > 0$, since 1 could not be represented if it were not itself an element of the basis. Also, an h -basis for $n > 0$ is clearly an h -basis for any non-negative number less than n . The set $\{0, 1, 3, 4\}$ is a minimal 2-basis for 8 . We prove this as follows: Along with 0 and 1 , any 2-basis requires either 2 or 3 , or else 3 could not be formed. The sets $\{0, 1, 2\}$ and $\{0, 1, 3\}$ are 2-bases for at most 4 (in fact, they are minimal 2-bases for 4). Since three elements do not suffice to form a 2-basis for $n \geq 5$, and $\{0, 1, 3, 4\}$ is a basis for 8 , this set is a minimal 2-basis for 8 . It is easily shown to be the only minimal 2-basis for 8 . It is also a minimal 2-basis for $5, 6$, and 7 , while $\{0, 1, 2, 5\}$, for example, is a minimal 2-basis for 7 but not for 8 .

We list some examples of $k_2(n)$, along with pertinent minimal bases on the right:

$$k_2(0) = 1 \qquad 0$$

$$k_2(1) = k_2(2) = 2 \qquad 0, 1$$

$$k_2(3) = k_2(4) = 3 \qquad 0, 1, 2 \text{ or } 0, 1, 3$$

$$k_2(5) = k_2(6) = k_2(7) = k_2(8) = 4 \qquad 0, 1, 3, 4$$

$$k_2(9) = \dots = k_2(12) = 5 \qquad 0, 1, 3, 5, 6 .$$

Generally, $k_h(0) = 1$, $k_h(1) = \dots = k_h(h) = 2$, $k_h(h+1) = 3$.

What is desired, of course, is a method for writing down a minimal h -basis for any given n . This has not been done for $h > 1$. Rohrbach gives a construction for an h -basis for given n , but it has not been shown that this basis is minimal. There is known no expression that gives $k_h(n)$ in terms of n (for $h \geq 2$). Given h and n , a minimal basis, and hence $k_h(n)$, could be found by investigating the $\binom{n+1}{r}$ r -combinations of the numbers $0, 1, \dots, n$ for $r = 0, 1, 2$, and so on until the first set that is an h -basis for n were found. Noting that the number of h -combinations with repetition of r numbers is $\binom{r+h-1}{h}$, and that if r numbers form an h -basis for n , then there must be at least $n+1$ of these combinations, we see that

$$(1.1) \qquad \binom{r+h-1}{h} \geq n+1 .$$

Hence, instead of starting with $r = 0$ above, we could start with the value of r just large enough to give this inequality. This method is of course impracticable. The best that has been done is to find upper and lower estimates for $k_h(n)$ (see the end of § 3, this chapter).

We shall deal mostly with the case $h = 2$. In § 2 we obtain an improvement of a lower bound for $k_2(n)$ found by Moser [21]. In § 3 we consider the function $n_h(k)$, which is the largest integer for which an h -basis of k elements exists. It is, in a sense, an inverse function of $k_h(n)$. We give the values of $n_2(k)$ for $k = 1, 2, \dots, 8$. Finally, in § 4 we discuss a notion in set theory that is analogous to that of bases for an integer.

2. Upper and lower estimates for $k_2(n)$.

We shall here consider bounds for $k_2(n)$. For convenience, we may write k or $k(n)$ in place of $k_2(n)$ in this section.

Let $A: a_1 < a_2 < \dots < a_k$ be a minimal 2-basis for n . We can form $\binom{k+1}{2}$ 2-combinations with repetition of elements of A . Since the set of the sums in pairs of the elements of A contains $0, 1, \dots, n$ (we consider a_i, a_i a pair, here), we have

$$(1.2) \quad \frac{k^2 + k}{2} \geq n + 1.$$

For $k \geq 5$, Rohrbach [26] showed that $k \geq \sqrt{2n}$. An upper estimate for k is found by noting that the numbers

$$(1.3) \quad 0, 1, 2, \dots, [\sqrt{n}-1], [\sqrt{n}], 2[\sqrt{n}], \dots, [\sqrt{n}][\sqrt{n}], [\sqrt{n}+1][\sqrt{n}]^{1)}$$

¹⁾ $[x]$ denotes the greatest integer not exceeding x .

form a 2-basis for n with $2 \lfloor \sqrt{n} \rfloor + 1$ elements. We show that this implies $k \leq 2 \sqrt{n}$ for $n \geq 1$. We will then have

$$(1.4) \quad \sqrt{2n} \leq k \leq 2 \sqrt{n} ,$$

or, in another form,

$$(1.4a) \quad \frac{k^2}{2} \left(1 - \frac{1}{2}\right) \leq n \leq \frac{k^2}{2} ,$$

provided $k \geq 5$. The set (1.3) is a 2-basis for

$\lfloor \sqrt{n} + 1 \rfloor \lfloor \sqrt{n} \rfloor + \lfloor \sqrt{n} \rfloor$, which may be larger than n . Using (1.3), we can form the numbers up to $\lfloor \sqrt{n} \rfloor^2 + \lfloor \sqrt{n} \rfloor$ with only the first $2 \lfloor \sqrt{n} \rfloor$ terms. Hence, if $n \leq \lfloor \sqrt{n} \rfloor^2 + \lfloor \sqrt{n} \rfloor$, the number of elements of (1.3) required to form a 2-basis for n is less than $2 \sqrt{n}$. To form the numbers $\lfloor \sqrt{n} \rfloor^2 + \lfloor \sqrt{n} \rfloor + 1$ up to $\lfloor \sqrt{n} + 1 \rfloor \lfloor \sqrt{n} \rfloor + \lfloor \sqrt{n} \rfloor$, using (1.3), requires all $2 \lfloor \sqrt{n} \rfloor + 1$ elements. If $n \geq \lfloor \sqrt{n} \rfloor^2 + \lfloor \sqrt{n} \rfloor + 1$, then $n > \lfloor \sqrt{n} \rfloor^2 + \lfloor \sqrt{n} \rfloor + \frac{1}{4}$; multiplying through by 4 and taking square roots yields $2 \sqrt{n} > 2 \lfloor \sqrt{n} \rfloor + 1$. Hence, in any case, the number of elements required in a 2-basis for n is less than $2 \sqrt{n}$. This does not hold if $n = 0$, since $k(0) = 1$.

I. Schur had conjectured that $k = O(\sqrt{n})$, and this was proved correct by Rohrbach, who in turn conjectured that

$$(1.5) \quad k^2 \sim 4n , \quad \text{or} \quad \frac{k^2}{2} \left(1 - \frac{1}{2}\right) \sim n .$$

He proved the much weaker statement $\frac{k^2}{2}(1 - .0016) > n$ for n sufficiently large. This result was improved upon by Moser [21], who showed that $\frac{k^2}{2}(1 - .0197) > n$ for n large. We show here, using a method similar to that of Moser, that

$$(1.6) \quad \frac{k^2}{2} (1 - .0269) > n .$$

First consider the generating function

$$(1.7) \quad f(x) = \sum_{j=1}^k x^{a_j}$$

and the function

$$(1.8) \quad g(x) = \frac{f^2(x) + f(x^2)}{2} .$$

The function $f^2(x)$ consists of $2 \binom{k}{2}$ terms with exponents $a_i + a_j$ ($i, j = 1, \dots, k$; $i \neq j$) and k terms with exponents $2a_i$ ($i = 1, \dots, k$). Hence the exponents that appear in $g(x)$ are all the sums in pairs of the elements of A . Therefore the coefficient of x^r in $g(x)$ is the number of representations of r in the form $a_s + a_t$, order not taken into account. Since A is a 2-basis for n , this coefficient is at least one for $r = 0, 1, \dots, n$, and we can write

$$(1.9) \quad g(x) = 1 + x + \dots + x^n + \sum_{r=0}^{2a_k} \delta(r) x^r ,$$

where $\delta(r) \geq 0$. Putting $x = 1$ here yields

$$(1.10) \quad \frac{k^2 + k}{2} = n + 1 + \sum \delta(r),$$

which implies (1.2). We wish to show that $\frac{k^2 + k}{2}$ exceeds $n + 1$ by a substantial amount, and to do this we show that $\sum \delta(r)$ is large.

For $x = e^{\frac{2\pi it}{n+1}}$, where t is a positive integer not divisible by $n + 1$, the expression $1 + x + \dots + x^n$ in (1.9) vanishes. Let $x_t = e^{\frac{2\pi it}{n+1}}$; we shall consider the cases $t = 1, 2$, and 4 . From (1.9) follows

$$|g(x_1)| = \left| \sum \delta(r) e^{\frac{2\pi ir}{n+1}} \right| \leq \sum \delta(r).$$

Thus

$$\begin{aligned} \sum \delta(r) &\geq \frac{1}{2} \left| f^2(x_1) + f(x_1^2) \right| \\ &= \frac{1}{2} \left| \left(\sum_{j=1}^k e^{\frac{2\pi i a_j}{n+1}} \right)^2 + \sum_{j=1}^k e^{\frac{4\pi i a_j}{n+1}} \right| \\ &\geq \frac{1}{2} \left\{ \left| \sum_{j=1}^k e^{\frac{2\pi i a_j}{n+1}} \right|^2 - \left| \sum_{j=1}^k e^{\frac{4\pi i a_j}{n+1}} \right| \right\} \\ &\quad \text{(by the triangle inequality)} \\ &\geq \frac{1}{2} \left\{ \left| \sum_{j=1}^k e^{\frac{2\pi i a_j}{n+1}} \right|^2 - k \right\} \\ (1.11) \quad &\geq \frac{1}{2} \left\{ \left(\sum_{j=1}^k \sin \frac{2\pi a_j}{n+1} \right)^2 - k \right\}. \end{aligned}$$

The use of x_2 and x_4 similarly yields

$$(1.12) \quad \sum \delta(r) \geq \frac{1}{2} \left\{ \left(\sum_{j=1}^k \cos \frac{4\pi a_j}{n+1} \right)^2 - k \right\}$$

and

$$(1.13) \quad \sum \delta(r) \geq \frac{1}{2} \left\{ \left(\sum_{j=1}^k \cos \frac{8\pi a_j}{n+1} \right)^2 - k \right\} .$$

Let $\theta_j = \frac{2\pi a_j}{n+1}$; it is clear that $0 < \theta_j < 2\pi$.

Consider the function $y(\theta) = \sin \theta + v \cos 2\theta + u \cos 4\theta$,
where θ is continuous and v and u are independent of θ
and between zero and one. For certain values of v and u ,
 $y(\theta)$ will have a positive minimum α on $[0, \pi]$ and a negative
minimum $-\beta$ on $[\pi, 2\pi]$ (see Figs. 1, 2). Let p be the number
of elements of A that exceed $\left[\frac{n+1}{2} \right]$. (The restriction $p = 0$
allows a better result than that obtained with $p > 0$.) Then,
for such values of v and u , it is easily seen that

$$(1.14) \quad \sum_{j=1}^k (\sin \theta_j + v \cos 2\theta_j + u \cos 4\theta_j) \geq \alpha(k-p) - \beta p ,$$

whence

$$(1.15) \quad \max \left(\sum_{j=1}^k \sin \theta_j, \sum_{j=1}^k \cos 2\theta_j, \sum_{j=1}^k \cos 4\theta_j \right) \geq \frac{\alpha k - (\alpha + \beta) p}{1 + v + u} .$$

Hence, by (1.11) , (1.12) and (1.13),

$$(1.16) \quad \sum \delta(r) \geq \frac{1}{2} \left\{ \left(\frac{\alpha k - (\alpha + \beta) p}{1 + v + u} \right)^2 - k \right\} .$$

Furthermore, there are $\binom{p+1}{2}$ pairs (i.e. 2-combinations with repetition) of a's which are greater than $\left\lfloor \frac{n+1}{2} \right\rfloor$, and so there are at least this many pairs whose sums exceed n . Hence, from (1.9), we obtain

$$(1.17) \quad \sum \delta(r) \geq \frac{p^2 + p}{2} \geq \frac{p^2}{2} .$$

For convenience, we write $\mu = \frac{\alpha}{1 + v + u + \alpha + \beta}$. There are two cases to be considered: (i) $p < \mu k$; (ii) $p \geq \mu k$. For cases (i) and (ii) respectively, (1.16) and (1.17) yield the inequality

$$(1.18) \quad \sum \delta(r) \geq \frac{k^2}{2} \mu^2 - \frac{k}{2} .$$

By (1.10) and (1.18),

$$(1.19) \quad \frac{k^2}{2} (1 - \mu^2) + k \geq n + 1 .$$

For n large, this yields an inequality of the form (1.6).

The problem now is to find values of v and u which will maximize μ^2 . Of course, $\max \mu^2$ will be less than $\frac{1}{2}$, since if $\frac{k^2}{2} (1 - \eta) > n$, then $\eta < \frac{1}{2}$ because of (1.4a). For $v = .4$, $u = .15$, we obtain $\mu^2 = .0269$, giving (1.6) for n sufficiently large. (Fig. 1 is the graph of $y(\theta)$ with $v = .4$, $u = .15$.) While it is doubtless possible to obtain a better result by using some other values of v and u , the improvement over (1.6) may not be such as to warrant the effort.

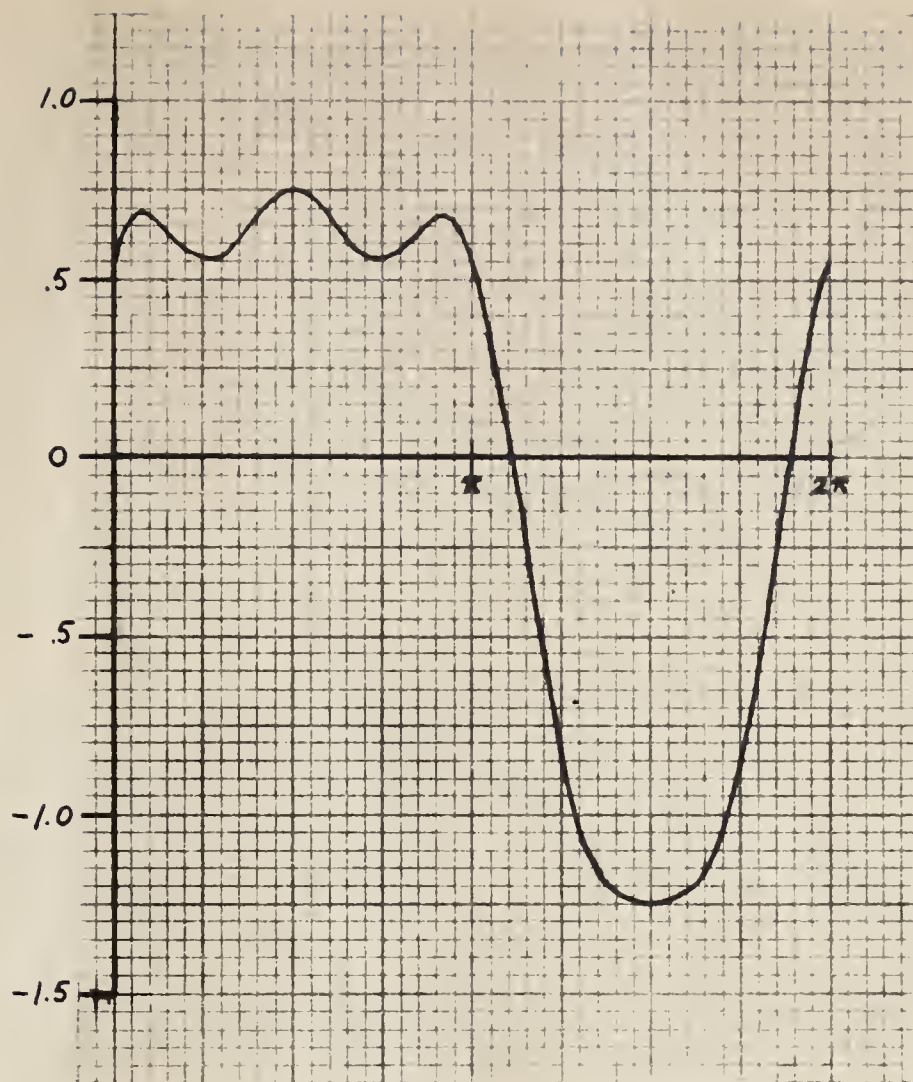


Figure 1.

The graph of

$$y(\theta) = \sin \theta + v \cos 2\theta + u \cos 4\theta \quad (0 \leq \theta \leq 2\pi)$$

with $v = .4$, $u = .15$. The minimum that appears near $\theta = \frac{\pi}{4}$ is greater than .5537, hence $\alpha = v + u = .55$, this value of $y(\theta)$ occurring at $\theta = 0$ and at $\theta = \pi$. Since $y''\left(\frac{3\pi}{2}\right) > 0$, the minimum in the interval $[\pi, 2\pi]$ is $y\left(\frac{3\pi}{2}\right) = -(1 + v - u)$, whence $\beta = 1.25$.

It would seem that the most that could be hoped for is an increase in the third decimal place of μ^2 , a trivial improvement.

Through the use of more roots of unity x_t , and hence of a different $y(\theta)$, one should be able to obtain a better result than (1.6). Also, a more critical examination of the ranges on $[0, 2\pi]$ in which certain minima of $y(\theta)$ are obtained, coupled with some consideration of the possible distribution of the elements of minimal bases, should yield a better result. (In obtaining his result, Rohrbach did, to some extent, consider distribution.)

The restricted case in which $p = 0$. Here, we define a restricted 2-basis for n to be a 2-basis for n in which the largest element is $\left\lfloor \frac{n+1}{2} \right\rfloor$, and let k be the minimal number of elements necessary in such a basis. We let

$$A : a_1 = 0 < a_2 = 1 < a_3 < \dots < a_k = \left\lfloor \frac{n+1}{2} \right\rfloor$$

be a minimal restricted 2-basis for n . This case allows us a better result than did the general case dealt with above. That is, the lower bound for k can be raised farther.

As before (see (1.4)), we have the lower estimate $\sqrt{2n}$ for k . Rohrbach [26] showed that the upper estimate in (1.4) holds for this case as well, and we give the proof of this. First we state the following result of Rohrbach: For every pair of positive integers x, y , the set

$$\begin{aligned}
 & 0, 1, 2, \dots, x-1, \\
 (1.20) \quad & 2x-1, 3x-1, \dots, (y+1)x-1, \\
 & (y+2)x-1, (y+2)x, \dots, (y+3)x-2
 \end{aligned}$$

is a 2-basis of $2x+y$ elements for the number

$$2(y+3)x - 4 = 2xy + 6x - 4.$$

This is easily seen, and we omit the proof. Now, if $m > 1$, and we put

$$(1.21) \quad x = \left[\frac{m+4}{4} \right]$$

and

$$(1.22) \quad y = m - 2 \left[\frac{m+4}{4} \right],$$

then (1.20) forms a 2-basis for

$$n = 2xy + 6x - 4 = \frac{m^2}{4} + \frac{3}{2}m - \gamma$$

where $\gamma = 2, \frac{7}{4}, 2$, or $\frac{11}{4}$ according as $m \equiv 0, 1, 2$, or $3 \pmod{4}$.

Now let $n > 1$ be given, and let m be the smallest integer such that

$$(1.23) \quad \frac{m^2}{4} + \frac{3}{2}m - \frac{11}{4} \geq n.$$

Then, if x and y are chosen in accordance with (1.21) and (1.22), (1.20) forms a 2-basis for n . By the definition of m in (1.23),

$$\frac{(m-1)^2}{4} + \frac{3}{2} (m-1) - \frac{11}{4} < n ,$$

whence

$$m^2 + 4m - 16 < 4n ,$$

and

$$(1.24) \quad m < 2\sqrt{n+5} - 2 \leq 2\sqrt{n}$$

for $n \geq 4$. For $n = 2$ and 3 , it is easy to show directly that there exist 2-bases with fewer than $2\sqrt{n}$ elements.

We give the following example: For $n = 100$, we find from (1.24) that $m < 2\sqrt{105} - 2 < 18.6$. Hence, with $m = 18$, we have $x = 5$, $y = 8$. The basis (1.20) becomes:

0, 1, 2, 3, 4, 9, 14, 19, 24, 29, 34, 39, 44, 49, 50, 51, 52, 53.

This is a 2-basis for 106 as well. For any $n > 1$, we can assure that the largest element in the basis is $\left\lceil \frac{n+1}{2} \right\rceil$ as follows: Let $b_1, b_2, \dots, b_m$ be the basis yielded by (1.20), (1.21), and (1.22). We reduce by $b_m - \left\lceil \frac{n+1}{2} \right\rceil$ all elements that exceed $\left\lceil \frac{b_m+1}{2} \right\rceil$. Thus, for $n = 100$, we have the basis

0, 1, 2, 3, 4, 9, 14, 19, 24, 26, 31, 36, 41, 46, 47, 48, 49, 50.

Rohrbach proved that, for n sufficiently large,

$$\frac{k^2}{2} (1 - .0692) > n ,$$

which is closer to his conjecture (1.5) than the inequalities

obtained in the general case. Moser [22] has shown that $\frac{k^2}{2} (1 - \frac{1}{q}) > n$. We shall obtain a further improvement below.

We use the method and notation employed in the general case. We define the functions (1.7) and (1.8) for the restricted basis A , and then (1.9) to (1.13) all hold. If θ_j is defined on the restricted basis A (so that $0 \leq \theta_j \leq \pi$), then for certain values of v and u , (1.14), (1.15), and (1.16) hold with $p = 0$. Hence, from (1.16), we obtain

$$\sum_{r=0}^{2a_k} \delta(r) \geq \frac{1}{2} \left\{ \left(\frac{\alpha k}{1 + v + u} \right)^2 - k \right\}.$$

We write $\gamma = \frac{\alpha}{1 + v + u}$, for convenience. Then, by (1.10) and the last inequality, we have

$$\frac{k^2}{2} (1 - \gamma^2) + k \geq n + 1,$$

which, for sufficiently large n , yields

$$\frac{k^2}{2} (1 - \gamma^2) > n.$$

Now (see Fig. 2, for example), either $\alpha = y(0)$ ($= v + u$) or $\alpha = y(M)$, where M is a point in $(0, \pi]$ at which a local minimum of $y(\theta)$ occurs. Since $y(\theta)$ is symmetrical about $\theta = \frac{\pi}{2}$ in the interval $[0, \pi]$, we can confine our discussion to the interval $[0, \frac{\pi}{2}]$, and choose M to be in this interval. Consider the following two cases:

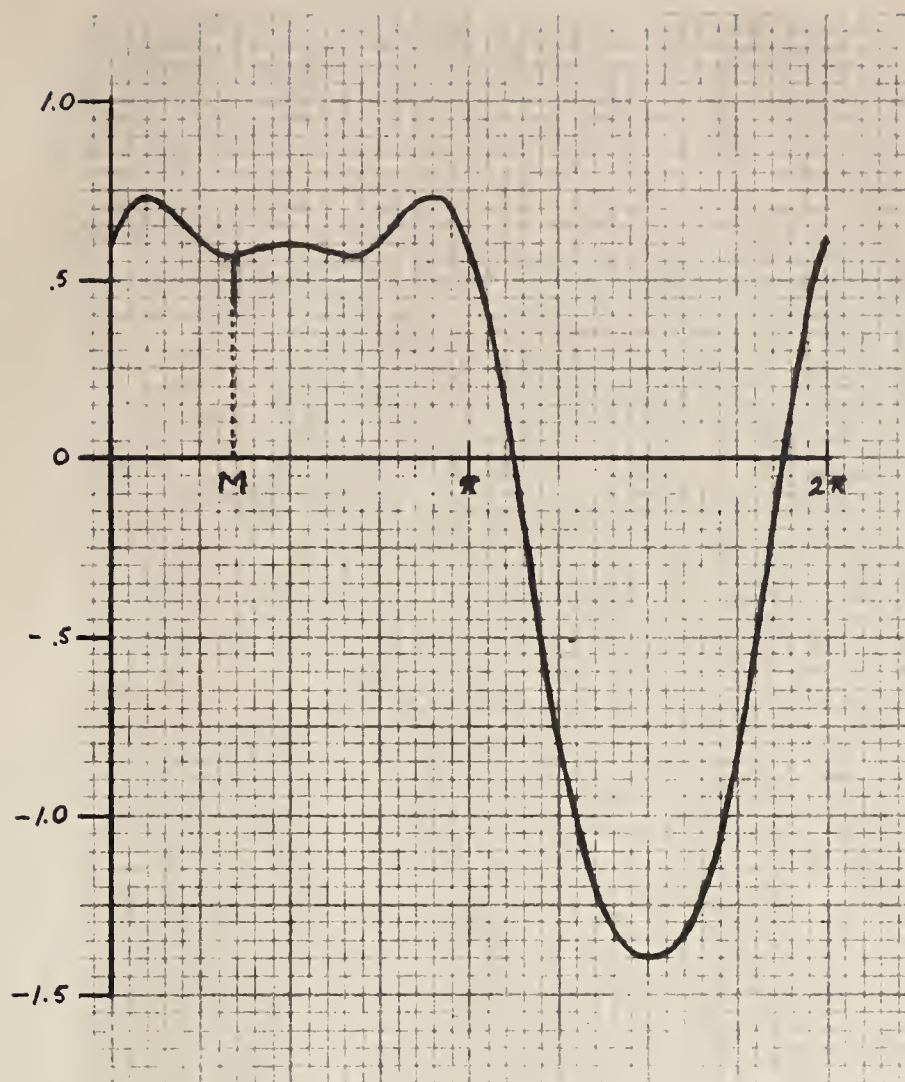


Figure 2.

The graph of

$$y(\theta) = \sin \theta + v \cos 2\theta + u \cos 4\theta \quad (0 \leq \theta \leq 2\pi)$$

with $v = .5$, $u = .1$. For these values of v and u , M is approximately $\frac{61.55 \pi}{180}$, and $y(M) < .5659$.

(i) $y(0) < y(M)$; (ii) $y(0) > y(M)$.

(i) Here, $\alpha = y(0)$, and hence

$$\gamma = \frac{y(0)}{1 + y(0)} .$$

Since the expression $\frac{a}{1 + a}$ increases with increasing a , we see that γ will be increased if v and u are altered so that $y_1(0) = y_1(M_1)$. M_1 is the point in $\left[0, \frac{\pi}{2}\right]$ at which the local minimum of $y_1(\theta)$ occurs.

(ii) Here, $\alpha = y(M)$, and hence

$$\gamma = \frac{y(M)}{1 + y(0)} .$$

Consider v and u as being altered so that $y(M)$ is increased to $y_2(M_2) = y_2(0)$. We must consider two sub-cases. First, suppose that $y_2(0) < y(0)$. Then $\frac{1}{1 + y(0)} < \frac{1}{1 + y_2(0)}$, and since $y(M) < y_2(M_2)$,

$$\frac{y(M)}{1 + y(0)} < \frac{y_2(M_2)}{1 + y_2(0)} .$$

Hence γ is increased in this sub-case. Second, suppose that $y_2(0) > y(0)$. Then

$$\frac{y_2(0)}{1 + y_2(0)} > \frac{y(0)}{1 + y(0)} > \frac{y(M)}{1 + y(0)} ,$$

and γ is increased again. Therefore, in either case (i) or

case (ii), ν can be increased. Hence, for the maximal value of ν , we shall have

$$(1.25) \quad y(0) = y(M) .$$

Now we note that for a given value of v , $y(M)$ is largest if u is chosen so that $M = \frac{3\pi}{8}$, since $y(M) < y\left(\frac{3\pi}{8}\right)$ if $M \neq \frac{3\pi}{8}$. Therefore, the optimal values for v and u satisfy

$$(1.26) \quad y'\left(\frac{3\pi}{8}\right) = \cos \frac{3\pi}{8} - 2v \sin \frac{3\pi}{4} - 4u \sin \frac{3\pi}{2} = 0 .$$

Re-writing (1.25) and (1.26), with $M = \frac{3\pi}{8}$ in (1.25), we obtain, respectively,

$$v + u = .92388 - \frac{\sqrt{2}}{2} v$$

and

$$.38268 - \sqrt{2} v + 4u = 0 .$$

Solving these equations for v and u yields

$$v = .49477 , \quad u = .07925 .$$

Then $\nu = \frac{v + u}{1 + v + u} = \frac{.57402}{1.57402}$; since the last figure is

in doubt, we may drop it, but we have, at least, $\nu > \frac{.574}{1.574}$.

Hence $\nu^2 > .13298$, and for n sufficiently large,

$$\frac{k^2}{2} (1 - .1329) > n .$$

Moser [22] has shown that a further improvement can be obtained if we require that A satisfy the condition

$$(1.27) \quad a_i + a_{k-i+1} = a_k = \left[\frac{n+1}{2} \right] .$$

The 2-basis (1.20) has this symmetry; hence, it might be expected that we should obtain a larger lower bound under this condition.

We proceed to obtain this improvement. Let $h(r)$ be the number of representations of r as the sum of two a 's, with repetitions allowed and order not taken into account. Then, since

$$\sin a_i x \cos a_j x + \cos a_i x \sin a_j x = \sin (a_i + a_j) x$$

and $2 \sin a_i x \cos a_i x = \sin 2 a_i x$, we have

$$\begin{aligned} & \left(\sum_{i=1}^k \sin a_i x \right) \left(\sum_{i=1}^k \cos a_i x \right) + \sum_{i=1}^k \sin a_i x \cos a_i x \\ &= \sum_{\substack{1 \leq i \leq k \\ i < j \leq k}} (\sin a_i x \cos a_j x + \cos a_i x \sin a_j x) + \sum_{i=1}^k \sin 2 a_i x \\ &= \sum_{r=0}^{2a_k} h(r) \sin r x . \end{aligned}$$

Let $\delta(r)$ have the same meaning as before. Then since A is a 2-basis for n , it follows that

$$\begin{aligned} & \left(\sum_{i=1}^k \sin a_i x \right) \left(\sum_{i=1}^k \cos a_i x \right) + \sum_{i=1}^k \sin a_i x \cos a_i x \\ &= \sum_{r=0}^n \sin r x + \sum_{r=0}^{2a_k} \delta(r) \sin r x \end{aligned}$$

(cf. (1.9)). We shall show that, for some value of x , $\sum_{r=0}^n \sin r x$ is positive and large, while the left hand side here is at most $\frac{k}{2}$. Then, from

$$\begin{aligned} (1.28) \quad \sum_{r=0}^{2a_k} \delta(r) &\geq \left| \sum_{r=0}^{2a_k} \delta(r) \sin r x \right| \\ &= \left| \sum_{r=0}^n \sin r x - \left(\sum_{i=1}^k \sin a_i x \right) \left(\sum_{i=1}^k \cos a_i x \right) - \sum_{i=1}^k \sin a_i x \cos a_i x \right|, \end{aligned}$$

it will follow that $\sum \delta(r)$ is large.

First, we note that

$$(1.29) \quad \sum_{r=0}^n \sin r x = \frac{\sin \frac{nx}{2} \sin \frac{(n+1)x}{2}}{\sin \frac{x}{2}}.$$

There are two cases to consider: (i) n odd; (ii) n even.

(i) Put $x = \frac{3\pi}{n+1}$. Then, by (1.29)

$$\sum_{r=0}^n \sin r x = \cot \frac{3\pi}{2(n+1)}.$$

For $n \geq 7$, $\tan \frac{3\pi}{2(n+1)} < \frac{3\pi}{2n}$, and hence

$$(1.30) \quad \sum_{r=0}^n \sin r x > \frac{2n}{3\pi}.$$

Also, since $a_k = \frac{n+1}{2}$, it follows from (1.27) that
 $a_i x + a_{k-i+1} x = \frac{3\pi}{2}$, whence $\sin a_i x = -\cos a_{k-i+1} x$ for
 $i = 1, \dots, k$. Hence

$$(1.31) \quad \left(\begin{array}{c} k \\ \sum_1 \sin a_i x \end{array} \right) \left(\begin{array}{c} k \\ \sum_1 \cos a_i x \end{array} \right) \leq 0 .$$

We have also

$$(1.32) \quad -\frac{k}{2} \leq \sum_1^k \sin a_i x \cos a_i x = \sum_1^k \frac{\sin 2 a_i x}{2} \leq \frac{k}{2} .$$

From (1.28), (1.30), (1.31), and (1.32) we obtain

$$\sum \delta(r) \geq \frac{2n}{3\pi} - \frac{k}{2} .$$

(ii) Put $x = \frac{3\pi}{n}$. Then (1.29) yields

$$\sum_{r=0}^n \sin r x = \cot \frac{3\pi}{2n} ,$$

from which, for $n \geq 8$, it follows that

$$\sum_{r=0}^n \sin r x > \frac{2(n-1)}{3\pi} .$$

In this case, $a_k = \frac{n}{2}$, and (1.31) and (1.32) follow as in case (i). We obtain

$$(1.33) \quad \sum \delta(r) \geq \frac{2(n-1)}{3\pi} - \frac{k}{2} > .212206 (n-1) - \frac{k}{2} .$$

Clearly, we can assert (1.33) in either case. For $n > 1061$, it follows from (1.33) that

$$\sum \delta(r) > .212 n - \frac{k}{2}.$$

Then, from (1.10) follows

$$(1.34) \quad \frac{k^2}{2} + k > 1.212 n.$$

For n sufficiently large, this yields

$$(1.35) \quad \frac{k^2}{2} (1 - .1749) > n.$$

Remark: While we have made several statements like this last one, we have never indicated how large n should be. We include this information for this case. By (1.24), $k \leq 2\sqrt{n}$; hence, (1.34) implies

$$\frac{k^2}{2n} > 1.212 - \frac{2}{\sqrt{n}}.$$

Re-writing (1.35), we obtain, on the other hand,

$$\frac{k^2}{2n} > \frac{1}{.8251} = 1.211962 \dots$$

If $1.212 - \frac{2}{\sqrt{n}} \geq 1.21197$, then n is sufficiently large; that is, it suffices that $n \geq \frac{4}{9} \times 10^{10}$.

3. The function $n_h(k)$.

The study of the function $k_h(n)$ can be related to that of another function; Let h and k be given positive

integers. Then, by $n_h(k)$ is meant the largest integer n for which there exists a set A of k integers

$$(1.36) \quad a_1 = 0 < a_2 = 1 < a_3 < \dots < a_k$$

such that each of the numbers $0, 1, \dots, n$ can be written as the sum of h summands from A .

Some remarks and examples follow.

While k numbers are sufficient to form an h -basis for $n_h(k)$, $k + 1$ numbers are required to form an h -basis for $n_h(k) + 1$. It follows that k is the minimal number of elements that can be used to form an h -basis for any of the integers $n_h(k-1) + 1$ up to $n_h(k)$. For example, we can see from the examples in §1 that $n_2(3) = 4$, since $\{0, 1, 2\}$ and $\{0, 1, 3\}$ are 2-bases for 4, but not for 5. It is easily seen that $n_2(4) = 8$, for, as we noted in §1, $\{0, 1, 3, 4\}$ is the only minimal 2-basis for 8, and this is not a 2-basis for 9. If $n_2(4)$ were 9, there would have to exist a 2-basis of four elements for 9, and such a basis would be a minimal 2-basis for 8.

The function $n_h(k)$ has, for $k \geq 2$, the monotonic properties $n_h(k+1) > n_h(k)$ and $n_{h+1}(k) > n_h(k)$. In a certain sense, it is the inverse function of $k_h(n)$: if $n_0 = n_h(k_0)$, then $k_h(n_0) = k_0$ and $k_h(n_0 + 1) = k_0 + 1$. For $k_h(n_0) > k_0$ implies that k_0 elements are insufficient to form an h -basis for n_0 , which is not so, and if $k_h(n_0) < k_0$, then

$n_h(k_h(n_0)) < n_h(k_0) = n_0$. But $k_h(n_0)$ numbers are by definition enough to form an h -basis for n_0 . The second part of the assertion is clear. On the other hand, if $k_1 = k_h(n_1)$, it does not follow that $n_h(k_1) = n_1$, but rather only that $n_h(k_1) \geq n_1$.

Before proceeding farther, we introduce the notion of an extremal basis. A set A of numbers (1.36) is called an extremal basis belonging to h and k if each of the numbers $0, 1, \dots, n_h(k)$ can be represented as the sum of h summands from A , or, in other words, if A is a minimal h -basis for $n_h(k)$.

Clearly, $n_h(1) = 0$; the only extremal basis for this case is $\{0\}$. $n_h(2) = h$, and the only extremal basis here is $\{0, 1\}$. Also, $n_1(k) = k-1$; the only extremal basis here is $\{0, 1, \dots, k-1\}$. We prove the following result of Stöhr [31] :

$$(1.37) \quad n_h(3) = \left[\frac{h^2 + 6h + 1}{4} \right] .^{2)}$$

(We also find all the extremal bases for the case.)

PROOF:

Let A be the set $\{0, 1, a\}$; the value of a determines for how large an integer n the set A will form a

²⁾ The k which Stöhr uses in his paper represents the number of positive integers in a basis A ; hence his k corresponds to our $k-1$. The LHS of this equation in his paper is $n_h(2)$.

basis. We require that $1 < a \leq h+1$, for if $a > h+1$, then h would be the largest number for which A would form an h -basis. Every integer in the interval $[0, (h-a+3)a-2]$ is representable as the sum of h summands from A . For consider the number $(h-a+1)a + a-1 = (h-a+2)a-1$. We can form all numbers up to and including this through the use of at most $(h-a+1)$ a 's and at most $(a-1)$ 1 's. Beyond this, we can form the numbers $(h-a+2)a$, $(h-a+2)a+1$, ..., $(h-a+2)a + a-2 = (h-a+3)a-2$ using at most $(h-a+2) + a-2 = h$ summands, but $(h-a+3)a-1$ cannot be so formed. Hence, $n_h(3)$ is equal to the largest value which

$$(h-a+3)a-2 = \frac{h^2 + 6h + 1}{4} - \left(a - \frac{h+3}{2}\right)^2$$

can have for suitably chosen a . Therefore, the integer a must be chosen as close as possible to $\frac{h+3}{2}$. If h is odd, there is the one extremal basis $\left\{0, 1, \frac{h+3}{2}\right\}$, and $n_h(3) = \frac{h^2 + 6h + 1}{4}$. If h is even, there are two extremal

bases, namely $\left\{0, 1, \frac{h+2}{2}\right\}$ and $\left\{0, 1, \frac{h+4}{2}\right\}$, and

$n_h(3) = \frac{h^2 + 6h}{4}$. In either case, (1.37) holds. There seem to be no further explicit expressions for $n_h(k)$ for unspecified h or for unspecified k .

Stöhr has compiled the following tables:

<u>h</u>	<u>k</u>	<u>$n_h(k)$</u>	<u>extremal A</u>
2	4	8	0, 1, 3, 4
2	5	12	0, 1, 3, 5, 6
2	6	16	0, 1, 3, 5, 7, 8
3	4	15	0, 1, 4, 5
3	5	24	0, 1, 4, 7, 8
4	4	26	0, 1, 5, 8

From this table, and from the remarks of the preceding paragraph, we obtain the following table of values of $n_h(k)$;

	k					
	1	2	3	4	5	6
1	0	1	2	3	4	5
2	0	2	4*	8	12	16
h 3	0	3	7	15	14	
4	0	4	10*	26		
5	0	5	14			

For the cases marked with an asterisk there are two extremal bases, and in each of the remaining cases there is one.

We have proved further that $n_2(7) = 20$ and $n_2(8) = 26$. Stöhr remarks, in the above mentioned paper, that it is not known whether there can be more than two extremal bases for a given pair h, k . It turns out that there are five for the case $h = 2, k = 7$, namely

$\{0, 1, 2, 5, 8, 9, 10\}$, $\{0, 1, 3, 5, 7, 9, 10\}$, $\{0, 1, 3, 4, 8, 9, 11\}$
 $\{0, 1, 3, 4, 9, 11, 16\}$, and $\{0, 1, 3, 5, 6, 13, 14\}$, and
that there are three for the case $h = 2$, $k = 8$, namely
 $\{0, 1, 2, 5, 8, 11, 12, 13\}$, $\{0, 1, 3, 4, 9, 10, 12, 13\}$,
and $\{0, 1, 3, 5, 7, 8, 17, 18\}$. It seems likely that for any
given $h \geq 2$, the number of extremal bases is unbounded over the
range of k .

It is interesting to note that there is one restricted
extremal basis having the form (1.20) for each value of k for
which $n_2(k)$ is known. We have $\{0, 1\}$ for 2, $\{0, 1, 2\}$ for 4,
those listed in the above table for 8, 12, and 16, $\{0, 1, 3, 5, 7, 9, 10\}$
for 20, and $\{0, 1, 2, 5, 8, 11, 12, 13\}$ for 26. It follows that
all n in the interval $1 \leq n \leq 26$ have minimal 2-bases of the
form (1.20) (or of the form (1.20) as altered in the example
following (1.24)). Also, since $n_2(8) = 26$, a set of nine
elements that is a 2-basis for some $n > 26$ would be a minimal
2-basis for n . Thus, $\{0, 1, 2, 5, 8, 11, 14, 15, 16\}$ and
 $\{0, 1, 3, 5, 7, 9, 10, 21, 22\}$ are minimal 2-bases for 32, and
the first of these has the form (1.20). If there were a minimal
2-basis of the form (1.20) for all $n > 0$, then Rohrbach's
conjecture (1.5) would be true. Of course, the problem of
finding $k_2(n)$ would then lose its interest, since the more basic
problem of finding a minimal 2-basis for any n would have been
solved. It seems likely that the above bases for 32 are extremal,
that is, that $n_2(32) = 9$, but we did not try to prove this.

We shall give here the proof that $n_2(7) = 20$ and

that the extremal bases for this case are the five sets given above. The proof for the case $h = 2$, $k = 8$ is similar but longer.

We proceed as follows: we consider all possible cases under the assumption $n_2(7) \geq 21$, and show that, however, there is no 2-basis for 21 with only seven elements. A substantial reduction can be made in the number of cases to be considered through our knowledge of $n_2(k)$ for $k < 7$. Since $n_2(6) = 16$, $k_2(16) = 6$, and we require at least six of the numbers in a 2-basis for 21 to be less than or equal to 16, otherwise we should be unable to form some number in the range 0 to 16. Similarly, since $n_2(5) = 12$ and $n_2(4) = 8$, we require at least five elements not exceeding 12 and at least four not exceeding 8. Now, if we were to have exactly six elements not exceeding 16, these six would have to be 0, 1, 3, 5, 7, 8, since these form the only extremal basis for 16. We should then require the number 17 in the basis, giving a set of seven elements that is a basis for only 18. Hence, none of the elements in a set of seven may exceed 16 if we wish the set to be a 2-basis for some $n \geq 19$. It follows from these remarks that if a set of seven elements is to be a 2-basis for 21 (or for 19 or 20), its distribution must be such that its elements fall into the three intervals of the table below with the frequencies indicated in at least one of the nine cases.

		Interval		
		$[0,8]$	$[9,12]$	$[13,16]$
Case	I a)	4	3	0
	b)	4	2	1
	c)	4	1	2
	II a)	5	2	0
	b)	5	1	1
	c)	5	0	2
	III a)	6	1	0
	b)	6	0	1
	IV	7	0	0

We eliminate the cases in order.

I. The four elements in the interval $[0,8]$ must be 0, 1, 3, and 4 since these form the only extremal basis for 8.

I. a) If the elements in the interval $[9,12]$ are

9, 10, 11, | 9, 10, 12, | 9, 11, 12, | 10, 11, 12,

then the largest number for which we have a basis is

15. | 16. | 16. | 8.

(There are four different statements here, the items between corresponding partitions being parts of the same statement.)

I. b) All possibilities in this case are considered in the following table, the third column giving the largest number

for which the respective seven elements form a basis:

Elements in [9,12]	Elements in [13,16]	
9,10	13	14
9,10	14	15
9,10	15	16
9,10	16	14
9,11	13	18
9,11	14	15
9,11	15	16
9,11	16	20
9,12	any one	10
10,11	"	8
10,12	"	8
11,12	"	8

I. c) There are just five elements in the interval $[0,12]$. If these were to form a basis for 12, they would have to be 0, 1, 3, 5, 6, since these numbers form the only extremal basis for 12. Since in case I four of the elements were to be 0, 1, 3, 4, this case does not yield even a basis for 12.

II. a) We consider two sub-cases, according as the three smallest of the five elements in $[0,8]$ are: (i) 0, 1, 2; (ii) 0, 1, 3.

(i) We must consider the 15 2-combinations of the remaining six numbers in $[0,8]$. For each of these combinations we must consider the six 2-combinations of the four numbers in $[9,12]$. We have, then, 90 sets of seven elements that are to be considered as possible 2-bases for 21. We present, and eliminate, all these possibilities by means of a 15 x 6 table below. An unbracketed number appearing in the table is the largest number less than 21 that cannot be formed from the pertinent set of seven elements. If the smallest number that cannot be formed from a certain set of seven elements is less than the minimum of the two numbers from $[9,12]$ in that set, that smallest number appears, enclosed in brackets, in the space corresponding to the set. It is easily seen, from the arrangement of the table, that if such a number cannot be formed in a certain space in the table, then it cannot be formed in any of the spaces to the right of that space in that row. Hence, dashes appear to the right of these bracketed entries to indicate that the rest of the cases in that row are eliminated. An asterisk in a space indicates that the pertinent seven elements form a 2-basis for 20, but not for 21. While all the quintuples of numbers in the 15 rows are to begin with 0, 1, and 2, we write these three only in the first row, it being understood that they belong with every pair in lower rows.

		Pairs of elements in $[9,12]$					
		9,10	9,11	9,12	10,11	10,12	11,12
Quintuples of elements in $[0,8]$	0, 1, 2, 3, 4	17	19	20	(9)	-	-
	3, 5	17	19	20	(9)	-	-
	3, 6	17	19	20	19	19	(10)
	3, 7	15	19	20	19	18	20
	3, 8	(7)	-	-	-	-	-
	4, 5	17	19	20	19	19	20
	4, 6	17	19	20	(9)	-	-
	4, 7	15	19	20	19	18	(10)
	4, 8	(7)	-	-	-	-	-
	5, 6	17	19	20	(9)	-	-
	5, 7	13	19	20	19	18	20
	5, 8	*	15	19	17	19	18
	6, 7	(5)	-	-	-	-	-
	6, 8	(5)	-	-	-	-	-
	7, 8	(5)	-	-	-	-	-

(ii) Here, we have 10 2-combinations of the five elements greater than 3 in $[0,8]$, and use a 10 x 6 table to present all possibilities. We eliminate these possibilities in the same way as before.

		Pairs of elements in $[9,12]$					
		9,10	9,11	9,12	10,11	10,12	11,12
Quintuples of elements in $[0,8]$	0, 1, 3, 4, 5	17	19	20	19	19	20
	4, 6	17	19	20	19	19	20
	4, 7	15	19	20	(9)	-	-
	4, 8	15	*	19	17	19	(10)
	5, 6	17	19	20	19	19	20
	5, 7	*	19	20	(9)	-	-
	5, 8	(7)	-	-	-	-	-
	6, 7	(5)	-	-	-	-	-
	6, 8	(5)	-	-	-	-	-
	7, 8	(5)	-	-	-	-	-

Thus, while there are three bases for 20 in case II a), there is none for 21.

II. b) We use the method of a), with the same sub-cases (i) and (ii). Here, however, we need 16 columns in the tables for the 16 combinations of two elements, one from $[9,12]$, the other from $[13,16]$. The rows remain as in a), and we leave out those which were completely blanked out. The column headings serve both tables.

(i)

Element from [9,12]	9	10	11	12
Element from [13,16]	13 14 15 16	13 14 15 16	13 14 15 16	13 14 15 16
0,1,2,3,4	20 20 20 15	(9) - - -	- - - -	- - - -
3,5	20 20 19 20	(9) - - -	- - - -	- - - -
3,6	20 19 20 20	18 19 19 15	(10) - - -	- - - -
3,7	19 20 20 20	19 19 19 15	19 20 20 20	(11) - - -
4,5	20 20 12 19	19 17 18 19	20 20 18 19	(11) - - -
4,6	20 19 20 19	(9) - - -	- - - -	- - - -
4,7	19 20 20 19	19 19 18 19	(10) - - -	- - - -
5,6	20 17 19 20	(9) - - -	- - - -	- - - -
5,7	19 20 19 20	19 18 19 19	19 20 19 20	(11) - - -
5,8	20 20 19 20	19 17 19 19	20 20 18 20	(11) - - -

(ii)

0,1,3,4,5	20 20 17 15	19 16 17 18	20 20 17 18	(11) - - -
4,6	20 19 20 14	18 19 17 18	20 19 20 18	(11) - - -
4,7	19 20 20 15	(9) - - -	- - - -	- - - -
4,8	20 20 20 15	19 19 17 15	(10) - - -	- - - -
5,6	20 16 19 20	17 18 19 18	20 18 19 20	20 16 19 20
5,7	19 20 19 20	(9) - - -	- - - -	- - - -

We see that there is a basis neither for 21 nor for 20 in this case.

II. c) There are only five elements not exceeding 12; hence, these must be 0, 1, 3, 5, 6. We then need either 13 and 14 in the basis, giving a basis for 20, or 13 and 15, giving a basis for only 16.

III. a) To form 21 as the sum of two numbers requires, from the interval $[9, 12]$, either 9 and 12 or 10 and 11. However, in this case we are allowed only one element in this interval.

III. b) If the element in $[13, 16]$ is

16,		15,		14,		13,
-----	--	-----	--	-----	--	-----

then to form 21, 20, 19, and 18 respectively we need

5, 4, 3, and 2		6, 5, 4, and 3		7, 6, 5, and 4		8, 7, 6, and 5
----------------	--	----------------	--	----------------	--	----------------

from the interval $[0, 8]$. 0 and 1 complete the set of seven, and we have a basis for only

10.		12.		2.		2.
-----	--	-----	--	----	--	----

IV. Since the largest element in the set of seven is 8 or less, the set could form a basis for at most 16.

Having found a 2-basis for 21 in none of the nine cases, it follows that $n_2(7) \leq 20$. Since five sets of seven numbers were found to be 2-bases for 20, we have $n_2(7) = 20$. To show that these five sets are the only extremal bases for 20, we have only to alter the above arguments slightly. The arguments in I, II, and IV remain the same, yielding five extremal bases. The argument in III is as follows (we wish to show that there is no 2-basis for 20 in the two cases under III):

a) If the element in $[9,12]$ is 12, then to form 20, 19, 18, and 17 respectively we need 8, 7, 6, and 5. 0 and 1 complete the set of seven, and we have a basis for only 2. If the element in $[9,12]$ is 11, 10, or 9, then we could not form, respectively, 20, 19, or 20 (among other numbers, possibly).

b) If the element in $[13,16]$ is 16, then to form 20, 19, and 18 we need respectively 4, 3, and 2 from the interval $[0,8]$. With 0 and 1 we have six elements. Now to form 15 we need both 7 and 8, leaving us with at least one element too many. If the element in $[13,16]$ is

$$15, \quad | \quad 14, \quad | \quad 13,$$

then to form 20, 19, 18, and 17, we need

$$5, 4, 3, \text{ and } 2. \quad | \quad 6, 5, 4, \text{ and } 3. \quad | \quad 7, 6, 5, \text{ and } 4.$$

0 and 1 complete the set of seven, and we have a basis for at most

$$10. \quad | \quad 12. \quad | \quad 2.$$

Further knowledge of $n_h(k)$ seems to be only in the form of estimates from above and below. Rohrbach [26] shows that

$$(1.38) \quad \left(\frac{k}{h}\right)^h < n_h(k) < \binom{k+h-1}{h}.$$

Both inequalities hold for $h \geq 2$, $k \geq 2$. The argument used to prove the right hand inequality is quite similar to that used in proving (1.1). Proving the left hand inequality requires a basis construction which we shall not give here.

If, instead of the number k of elements in a basis we are given the integer n and seek an h -basis for it, we come back to the problem of finding $k_h(n)$. Rohrbach uses an intermediate step in the proof of the lower inequality in (1.38) to show that for $h \geq 3$, $k_h(n) < h \sqrt[h]{n}$, a generalization of the upper inequality in (1.4). Again, let n be given, and let $k_h(n) = k$. Then $n_h(k) \geq n$, whence from (1.38) we obtain $n < \binom{k+h-1}{h}$, a generalization of (1.2). Since $\frac{(k+h-1)^h}{h!} \geq \binom{k+h-1}{h}$, we have $\frac{k+h-1}{\sqrt[h]{n}} > \sqrt[h]{h!}$, and hence $\liminf_{n \rightarrow \infty} \frac{k}{\sqrt[h]{n}} \geq \sqrt[h]{h!}$. This corresponds to the lower inequality in (1.4), but of course, (1.4) held for all $k \geq 5$, hence for all $n \geq 7$.

4. An analogous problem in set theory.

The notion of h -bases for an integer has an analogue in set theory. Let a set S of n elements be given ($n \geq 1$). Denote the 2^n subsets of S by $S_1, S_2, \dots, S_{2^n}$, and let $\mathcal{A} = A_1, A_2, \dots, A_g$ be a subset of $\mathcal{S} = \{S_1, S_2, \dots, S_{2^n}\}$. We shall say that $\mathcal{A}$ is an h -basis for $\mathcal{S}$ if every subset S_i can be expressed in the form

$$(1.39) \quad A_{i_1} \cup A_{i_2} \cup \dots \cup A_{i_h}.$$

While in the case of bases for an integer we allowed repetitions

in the sums, here we do not allow any of the A_i in (1.39) to be repeated, except for the empty set E which must be in $\mathcal{U}$ if $\mathcal{U}$ is to be a basis. We let $k = k_h(n)$ be the smallest value of g for which $\mathcal{U}$ is an h -basis for $\mathcal{S}$. If $\mathcal{U}$ is an h -basis for $\mathcal{S}$ with k elements we call it a minimal h -basis for $\mathcal{S}$.

We shall deal with the case $h = 2$. Some examples of 2-bases are the following (let $S = \{1, 2, \dots, n\}$):

(i) Let $n = 4$. The set consisting of E , $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{1,2\}$, $\{3,4\}$ is a minimal 2-basis for $\mathcal{S}$.

(ii) Let $n = 5$. The sets E , $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{1, 2, 3\}$, $\{5\}$, $\{1,2\}$, $\{1,3\}$, $\{2,3\}$, $\{4,5\}$ form a 2-basis for $\mathcal{S}$ with 11 elements.

We give the following table of $k = k_2(n)$ for $n = 1, 2, 3, 4$:

(1.40)

n	1	2	3	4
k	2	3	5	7

If the basis in (ii) were minimal, then the first five values of $k_2(n)$ would be the first five primes.

Let $\mathcal{U}$ be a minimal 2-basis for $\mathcal{S}$. Corresponding to (1.4) we prove that

$$(1.41) \quad 2^{\frac{n+1}{2}} \leq k \leq 3 \cdot 2^{\frac{n-1}{2}}.$$

If n is even, the upper estimate here can be replaced by $2^{\frac{n+2}{2}}$.

This gives an analogy that is closer to (1.4) than is (1.41), namely

$$\sqrt{2 \cdot 2^n} \leq k \leq 2 \sqrt{2^n} ;$$

the place of the n in (1.4) is taken by 2^n here.

We proceed to prove the left hand inequality in (1.41). There are $\binom{k}{2}$ pairs of distinct subsets A_i , and one subset, E , is to be united with itself. Since the k subsets A_i do form a 2-basis for $\mathcal{C}$

$$\frac{k(k-1)}{2} + 1 \geq 2^n ,$$

or

$$k^2 - (k-2) \geq 2^{n+1} .$$

From the table (1.40), we see that $k - 2 \geq 0$ for all n . Hence

$$k \geq 2^{\frac{n+1}{2}} .$$

To prove the right hand inequality in (1.41), we consider the cases n even and n odd separately. If n is even, we divide S into two sets of $\frac{n}{2}$ elements each. These sets each have $2^{\frac{n}{2}}$ subsets. Clearly, every subset of S can be represented as the union of two of these $2 \cdot 2^{\frac{n}{2}}$ subsets. Hence $k \leq 2^{\frac{n+2}{2}}$. If n is odd, we split S into two sets, one with $\frac{n+1}{2}$ elements and one with $\frac{n-1}{2}$ elements. The $2^{\frac{n+1}{2}} + 2^{\frac{n-1}{2}}$ subsets of these form a 2-basis for $\mathcal{C}$, and hence $k \leq 3 \cdot 2^{\frac{n-1}{2}}$. Since $2^{\frac{n+2}{2}} < 3 \cdot 2^{\frac{n-1}{2}}$ for all n , (1.41) holds for all n .

Moser [23] proposed the problem of finding an improvement on the bounds in (1.41), but this has not been done.

CHAPTER II

BASES FOR THE INTEGERS

5. Introduction

We discuss in this chapter some results of Stöhr [31] and Cassels [3] concerning bases for the non-negative integers, defined immediately below.

Let $h \geq 1$. A subset B of the non-negative integers is called an h -basis, or a basis of order h , if every non-negative integer is representable as the sum of h numbers from B , repetitions being allowed. We sometimes use the expression " h -basis for the integers", or, when the meaning is clear, simply "basis". B is called an asymptotic h -basis if there is a positive integer N such that every integer greater than N is representable as the sum of h numbers from B , repetitions allowed.

We introduce some other customary notation. If A and B are sets of non-negative integers, then by their sum $A + B$ is meant the set of all numbers representable in the form $a + b$, where $a \in A$, $b \in B$. By hB is meant the sum $B + B + \dots + B$ with h equal summands. (Hence, B is an h -basis if hB is the set of all non-negative integers.) Finally, by $A(n)$, the counting function of A , is meant the number of non-zero integers in A which are less than or equal to n .

We discuss some examples: The only 1-basis is the set of the non-negative integers itself. The set $B = \{0, 1, h, 2h, 3h, \dots\}$ is an h -basis, albeit an inefficient one, since it has asymptotic density $\lim_{n \rightarrow \infty} \inf \frac{B(n)}{n} = \frac{1}{h}$. Most of the bases we shall consider in this chapter have asymptotic density zero. By Lagrange's theorem, the set of squares is a 4-basis, and this set has asymptotic density 0. Since $7 = 2^2 + 1^2 + 1^2 + 1^2$ is not representable as the sum of three squares, the squares do not form a 3-basis. Indeed, since no number of the form $8m + 7$ can be the sum of three squares (see Ch. XX, Hardy and Wright [15]), the squares do not form even an asymptotic 3-basis. On the other hand, the cubes form a 9-basis, and since only a finite number of integers require nine cubes (Hardy and Wright), they form an asymptotic 8-basis. That the k -th powers form a basis of finite order was conjectured by Waring [32] and first proved by Hilbert [16], [17]. As a last remark, we note that an h -basis is clearly an asymptotic h -basis, but the reverse is not necessarily true.

Stöhr (see § 6) investigated the ratio $\frac{B(n)}{\sqrt[n]{n}}$, which may be compared with the ratio $\frac{k_n(n)}{\sqrt[n]{n}}$ in the theory of h -bases for an integer n . Cassels (see § 7) proved that for $h = 2, 3, \dots$, there exists an h -basis B such that $\lim_{n \rightarrow \infty} \frac{b_n}{n^h}$ exists and is positive, where b_i is the $(i+1)$ -th element of B when B is ordered according to size. This proves a conjecture which Stöhr made in his paper concerning the possibility of constructing an h -basis for which $\lim_{n \rightarrow \infty} \frac{B(n)}{\sqrt[n]{n}}$ exists and is positive. For if

$$\lim_{n \rightarrow \infty} \frac{b_n}{n^h} = \gamma > 0, \text{ then } \lim_{n \rightarrow \infty} \frac{B(n)}{\frac{1}{\gamma} \sqrt[n]{n}} = \frac{1}{\gamma}.$$

6. On the ratio $\frac{B(n)}{\sqrt[n]{n}}$.

Let B be an h -basis. We use the following notation of Stöhr:

$$\beta_1 = \inf_{n=1,2,\dots} \frac{B(n)}{\sqrt[n]{n}},$$

$$\beta_2 = \lim_{n \rightarrow \infty} \inf \frac{B(n)}{\sqrt[n]{n}},$$

$$\beta_3 = \lim_{n \rightarrow \infty} \sup \frac{B(n)}{\sqrt[n]{n}},$$

$$\beta_4 = \sup_{n=1,2,\dots} \frac{B(n)}{\sqrt[n]{n}}.$$

The choice of the ratio $\frac{B(n)}{\sqrt[n]{n}}$ as an object of investigation seems reasonable in view of the following result of Rohrbach [26] :

For every positive integer h and every $\varepsilon > 0$, there is an h -basis B such that $B(n) < n^{\frac{1+\varepsilon}{h}}$ for all sufficiently large n . (Also see the discussion at the end of § 3, viewed in the light of (2.24) ahead.) It is clear that $0 \leq \beta_1 \leq \beta_2 \leq \beta_3 \leq \beta_4$, and that β_3 and β_4 may be infinite. By $\gamma_1(h)$, $\gamma_2(h)$, $\gamma_3(h)$, and $\gamma_4(h)$ we designate respectively the greatest lower bounds of β_1 , β_2 , β_3 , and β_4 when B runs through all h -bases.

Clearly $0 \leq \gamma_1(h) \leq \gamma_2(h) \leq \gamma_3(h) \leq \gamma_4(h)$. These four quantities will prove to be finite, and Stöhr shows that

$\gamma_1(h) = h^{-\frac{1}{h}}$, whence they are all positive. The quantities $\gamma_2(h)$, $\gamma_3(h)$, and $\gamma_4(h)$ have not been determined; only upper and lower estimates are known for them. Since for $h = 1$ the ratio $\frac{B(n)}{\sqrt[n]{n}}$ is one for all n , we shall consider only values of h greater than one in our discussion of these estimates, which follows immediately.

We proceed first to find lower estimates for $\gamma_2(h)$, $\gamma_3(h)$, and $\gamma_4(h)$.

Since the $B(n) + 1$ elements of B that are less than or equal to n form an h -basis for n , we have, from (1.1),

$$\binom{B(n) + h}{h} \geq n + 1.$$

We obtain from this a lower estimate for $\gamma_2(h)$:

$$\frac{(B(n) + h)^h}{h!} \geq \binom{B(n) + h}{h} > n,$$

$$B(n) + h > \sqrt[h]{h!} \sqrt[h]{n}.$$

Hence $\beta_2 \geq \sqrt[h]{h!}$ for any h -basis B , and therefore

$$\gamma_2(h) \geq \sqrt[h]{h!}.$$

For the case $h = 2$ we can obtain a better estimate through the use of (1.6). For sufficiently large n , we obtain from (1.6) the inequality $.4866 B^2(n) > n$. Hence

$$\beta_2 = \lim_{n \rightarrow \infty} \inf \frac{B(n)}{\sqrt{n}} \geq \frac{1}{\sqrt{.4866}}$$

holds for any 2-basis B , and therefore

$$\gamma_2(2) \geq \frac{1}{\sqrt{.4866}} > \sqrt{2}.$$

For $\gamma_3(h)$ we shall prove the following result of Stöhr:

$$(2.1) \quad \gamma_3(h) \geq \frac{\sqrt[h]{h!}}{\Gamma(1 + \frac{1}{h})}.$$

First we shall make some preliminary remarks and prove a lemma.

Let B be a given h -basis, N a given integer. If there exists a positive real number α (dependent on B and N) such that

$$(2.2) \quad B(n) \leq \alpha n^{\frac{1}{h}} \quad \text{for all } n \geq N,$$

then we shall prove that

$$(2.3) \quad \alpha \geq \frac{\sqrt[h]{h!}}{\Gamma(1 + \frac{1}{h})}.$$

Now, for some integer N_1 , $n \geq N_1$ implies

$$\beta_3 = \lim_{n \rightarrow \infty} \sup \frac{B(n)}{\sqrt[h]{n}} \geq \frac{B(n)}{\sqrt[h]{n}}, \quad \text{and hence } \beta_3 = \inf_N \alpha$$

for this given B . If there is no α such that (2.2) holds,

then $\frac{B(n)}{\sqrt[h]{n}} \rightarrow \infty$ as $n \rightarrow \infty$. It follows that for any h -basis B ,

$$(2.4) \quad \beta_3 \geq \frac{\sqrt[h]{h!}}{\Gamma(1 + \frac{1}{h})},$$

and (2.1) follows. Thus, to prove (2.1), it will suffice to prove that (2.3) holds under the assumption that there is an α such that (2.2) holds.

Since B is an h -basis, every integer $t \geq 0$ can be written in the form

$$(2.5) \quad t = b^{(1)} + b^{(2)} + \dots + b^{(h)} \quad (b^{(1)}, b^{(2)}, \dots, b^{(h)} \in B).$$

For every integer n we make the abbreviation $B(n) = k^{(1)}$ and denote by $m = m(n)$ the number of integers in the interval $[1, n]$ which cannot be written in the form (2.5) if

$$(2.6) \quad N \leq b^{(1)} < b^{(2)} < \dots < b^{(h)}.$$

We now state and prove the lemma.

LEMMA:

$$m \leq c B^{h-1}(n) \text{ for some constant } c.$$

PROOF:

Let M be the set of those integers in $[1, n]$ which cannot be written in the form (2.5) if (2.6) holds. Thus $\text{card } M$, the cardinal number of M , is m . Let M_1 be the set of

¹⁾ Note that because of the definition of a counting function, the k used here corresponds to $k-1$ in chapter I.

those integers in $[1, n]$ which cannot be written in the form

(2.5) if

$$(2.7) \quad N \leq b^{(1)} \leq b^{(2)} \leq \dots \leq b^{(h)} .$$

The elements of M_1 are among those numbers which are formed by allowing $b^{(1)}$ to run through the N numbers $0, 1, \dots, N-1$, and by allowing each of $b^{(2)}, \dots, b^{(h)}$ independently to run through the $k+1$ b 's in $[0, n]$. Letting $m_1 = \text{card } M_1$, we thus have

$$(2.8) \quad m_1 \leq N (k+1)^{h-1} .$$

We now consider the integers in $[1, n]$ that can be written in the form (2.5) if (2.7) holds, which form the complement of M_1 in the set $\{0, 1, 2, \dots, n\}$. Among these there is a set of integers that cannot be written in form (2.5) if (2.6) holds. Let this set be M_2 . It is clear that $M \subset M_1 \cup M_2$. If $m_2 = \text{card } M_2$, we thus have $m \leq m_1 + m_2$.

We have for m_2 :

$$(2.9) \quad m_2 \leq \binom{k - B(N-1) + h - 1}{h} - \binom{k - B(N-1)}{h} ,$$

for from the $k - B(N-1)$ b 's in $[N, n]$ there can be formed

$\binom{k - B(N-1) + h - 1}{h}$ h -combinations with repetition, hence that number of formally different sums of h summands, and among these there are $\binom{k - B(N-1)}{h}$ sums with all summands different.

The right hand side of (2.9) is a polynomial of degree not exceeding $h-1$ in k with coefficients that depend only on h and $B(N-1)$. Also, the right hand side of (2.8) is a polynomial of degree $h-1$ in k with coefficients depending only on h and N . For $n \geq 1$ we have $k \geq 1$. Hence, for $n \geq 1$, m satisfies

$$m \leq c k^{h-1} = c B^{h-1}(n) .^2)$$

We proceed with the proof of (2.3).

²⁾

This lemma replaces a part of Stöhr's proof which contains an error. He argues that $m \leq m_1 + m_2$, where m_1 is as above, but where m_2 is the number of integers in $[1, n]$ which cannot be written in the form (2.5) if $b^{(1)} < b^{(2)} < \dots < b^{(h)}$, and there is no other restriction on these b 's. It is possible to have a basis such that there are integers in $[1, n]$ which cannot be formed using different b 's restricted to be $\geq N$, but which can if the b 's are allowed to be less than N . Then it is possible that $m > m_1 + m_2$. A simple example with $h = 2$ is

$B : 0, 1, 2, 3, 5, 7, 9, \dots$ (all the remaining odd numbers).

Choosing $N = 10$ yields, for $n = 25$, say, $m = 24$, $m_1 = 23$, and $m_2 = 0$. The trouble here is that 22 can be written as the sum of two different b 's, but not as the sum of two different b 's greater than 10. For this B , Stöhr's m_2 is always zero.

From the lemma and (2.2) we obtain

$$(2.10) \quad m \leq c \alpha^{h-1} n^{1-\frac{1}{h}}.$$

Now, by summation over all sums (2.5) for which (2.6) holds,

$$n - m \leq \sum 1.$$

$$b^{(1)} + \dots + b^{(h)} \leq n$$

$$b^{(1)}, \dots, b^{(h)} \in B$$

$$N \leq b^{(1)} < b^{(2)} < \dots < b^{(h)}$$

The two sides here may be unequal since there may be more than one representation of an integer that can be written in form (2.5) when (2.6) holds. In the sums $b^{(1)} + \dots + b^{(h)}$ we permute the h pairwise different summands in all $h!$ ways, and then drop the restriction $b^{(1)} < b^{(2)} < \dots < b^{(h)}$, obtaining

$$(2.11) \quad h!(n-m) \leq \sum 1.$$

$$b^{(1)} + \dots + b^{(h)} \leq n$$

$$b^{(1)}, \dots, b^{(h)} \in B$$

$$N \leq b^{(1)}, \dots, N \leq b^{(h)}$$

Let $b_0 = 0 < b_1 < b_2 < \dots$ be the elements of B ordered according to size. Then, by (2.2), we have, for $b_r \geq N$,

$r = B(b_r) \leq \alpha b_r^{\frac{1}{h}}$, whence $b_r \geq r^h \alpha^{-h}$. In the summation condition of (2.11) we replace every b_r that occurs as one of $b^{(1)}, \dots, b^{(h)}$ by $r^h \alpha^{-h}$. The number of summands on the right hand side of (2.11) is not decreased if we sum over all non-negative integers $r_1, \dots, r_h$ for which $r_1^h \alpha^{-h} + \dots + r_h^h \alpha^{-h} \leq n$. This gives

$$(2.12) \quad h!(n-m) \leq \sum 1,$$

$$r_1^h \alpha^{-h} + \dots + r_h^h \alpha^{-h} \leq n$$

$$r_1, \dots, r_h \geq 0$$

or, after a simple transformation,

$$(2.13) \quad \frac{h!(n-m)}{\alpha^h n} \leq \sum \left(\frac{1}{\alpha n^{\frac{1}{h}}} \right)^h.$$

$$\frac{r_1^h}{\alpha^h n} + \dots + \frac{r_h^h}{\alpha^h n} \leq 1$$

$$r_1, \dots, r_h \geq 0$$

Since $\frac{n-m}{n} \geq 1 - \frac{c \alpha^{h-1}}{n^{\frac{1}{h}}}$ by (2.10), the left hand

side in (2.13) tends towards a limit not less than $\frac{h!}{\alpha^h}$ as $n \rightarrow \infty$. The right hand side tends towards the hyper-volume of that region in $(u_1, \dots, u_h)$ -space that is bounded through the inequalities $u_1^h + \dots + u_h^h \leq 1$, $u_1 \geq 0, \dots, u_h \geq 0$.

To see this we re-write the right hand side of (2.12):

$$\sum_{i=1}^h r_i^h \leq \alpha^h n$$

$$r_1^h + \dots + r_h^h \leq \alpha^h n$$

$$r_1, \dots, r_h \geq 0$$

This sum is equal to the number of lattice points in that region of the positive orthant in $(x_1, \dots, x_h)$ -space that is bounded by $x_1^h + \dots + x_h^h = \alpha^h n$. For consider the integers not exceeding $\alpha^h n$ that are representable as the sums of h -th powers of h non-negative integers $r_1, \dots, r_h$. Here, representations are regarded as distinct, even if they differ only in the order of $r_1, \dots, r_h$. (Hence, there can be as many as $h!$ representations of this kind of integer, and fewer if the r_i are not all distinct.) Each such representation of this kind of integer corresponds to a lattice point in the stated region, and each lattice point in this region corresponds to such an integer.

Now, with each of these lattice points we associate the unit hypercube that contains that lattice point and is such that the sum of the coordinates of that lattice point is less than the sum of the coordinates of any other point in the hypercube. We thus obtain a hyper-volume which is included in the region

$$(2.14) \quad x_1^h + \dots + x_h^h \leq (\alpha n^{\frac{1}{h}} + \sqrt{h})^h, \quad x_1 \geq 0, \dots, x_h \geq 0$$

and includes the region

$$(2.15) \quad x_1^h + \dots + x_h^h = (a n^{\frac{1}{h}} - \sqrt{h})^h, \quad x_1 \geq 0, \dots, x_h \geq 0. \quad ^3)$$

The hyper-volume of a region $H : x_1^h + \dots + x_h^h = a^h$,

$x_1 \geq 0, \dots, x_h \geq 0$ is $\int_H dx_1 \dots dx_h$. Putting

$y_i = \frac{x_i^h}{a^h}$ for $i = 1, \dots, h$, the hypersurface with which we

have to deal is transformed to $y_1 + \dots + y_h = 1$, and the

integral becomes

$$\begin{aligned} & \frac{a^h}{h^h} \int_0^1 \int_0^{1-y_h} \int_0^{1-y_{h-1}-y_h} \dots \int_0^{1-y_2-y_3-\dots-y_h} y_1^{\frac{1}{h}-1} \dots y_h^{\frac{1}{h}-1} dy_1 \dots dy_h \\ &= \frac{a^h}{h^{h-1}} \int_0^1 \dots \int_0^{1-y_3-\dots-y_h} (1-y_2-\dots-y_h)^{\frac{1}{h}} y_2^{\frac{1}{h}-1} \dots y_h^{\frac{1}{h}-1} dy_2 \dots dy_h. \end{aligned}$$

Through the repeated application of the formula

$$\int_0^{t_0} t^{p-1} (t_0 - t)^{q-1} dt = t_0^{p+q-1} B(p, q),$$

3) Re the use of $\sqrt{h}$ in (2.14) and (2.15); For a point $(x_1, \dots, x_h)$ on the hypersurface $x_1^h + \dots + x_h^h = a^h$, we may assume that $(x_1+1, \dots, x_h+1)$ is a point on another surface such that $(x_1+1)^h + \dots + (x_h+1)^h = p^h$. To justify the use of $\sqrt{h}$ instead of some other constant, we show that $p \leq a + \sqrt{h}$, or $p^h \leq a^h + \binom{h}{1} a^{h-1} h^{\frac{1}{2}} + \binom{h}{2} a^{h-2} h^{\frac{2}{2}} + \dots + h^{\frac{h}{2}}$. Expanding the terms $(x_i+1)^h$ of p^h yields

where $B(p,q)$ is the Beta-function of p and q , we find this integral to be

$$\frac{a^h}{h^{h-1}} B\left(\frac{1}{h}, \frac{1}{h} + 1\right) B\left(\frac{1}{h}, \frac{2}{h} + 1\right) \dots B\left(\frac{1}{h}, \frac{h-1}{h} + 1\right) = a^h \Gamma^h\left(1 + \frac{1}{h}\right).$$

Hence the regions (2.14) and (2.15) have respectively the volumes

$$\left(a n^{\frac{1}{h}} + \sqrt{h}\right)^h \Gamma^h\left(1 + \frac{1}{h}\right) \quad \text{and} \quad \left(a n^{\frac{1}{h}} - \sqrt{h}\right)^h \Gamma^h\left(1 + \frac{1}{h}\right).$$

It follows that

$$\begin{aligned} \sum_{i=1}^h r_i &= \left\{ a^h n + O\left(n^{\frac{h-1}{h}}\right) \right\} \Gamma^h\left(1 + \frac{1}{h}\right), \\ r_1^h + \dots + r_h^h &\leq a^h n \\ r_i &\geq 0, \dots, r_h \geq 0 \end{aligned}$$

and therefore the right hand side of (2.13) is

3) Cont'd.

$$p^h = a^h + \binom{h}{1} (x_1^{h-1} + \dots + x_h^{h-1}) + \binom{h}{2} (x_1^{h-2} + \dots + x_h^{h-2}) + \dots + h.$$

Since $x_1, \dots, x_h \leq a$, we have

$$x_1^{h-j} + \dots + x_h^{h-j} \leq h a^{h-j} \leq h^{\frac{j}{2}} a^{h-j} \quad \text{for } j = 2, \dots, h.$$

And the maximum of $x_1^{h-1} + \dots + x_h^{h-1}$, subject to the

condition $x_1^h + \dots + x_h^h = a^h$, is obtained for

$$x_1 = x_2 = \dots = x_h = \frac{a}{h^{\frac{1}{h}}}, \quad \text{and is therefore } h^{\frac{1}{h}} a^{h-1} \leq \sqrt{h} a^{h-1}$$

(we are considering only values of h greater than one).

The desired result follows.

$$\frac{1}{\alpha_n^h} \sum 1 = \Gamma^h \left(1 + \frac{1}{h}\right) + o\left(\frac{1}{n^{\frac{1}{h}}}\right).$$

$$\frac{r_1^h}{\alpha_n^h} + \dots + \frac{r_h^h}{\alpha_n^h} \leq 1$$

$$r_1, \dots, r_h \geq 0$$

As $n \rightarrow \infty$, this tends towards $\Gamma^h(1 + \frac{1}{h})$. It follows that

$$\frac{h!}{\alpha^h} \leq \Gamma^h \left(1 + \frac{1}{h}\right),$$

whence follows (2.3).

Remark: The assertion (2.4) holds also for sets B that are only asymptotic h -bases. For if $h B$ contains all integers greater than M , then clearly the union of B with $0, 1, 2, \dots, M$ is an h -basis, and thus (2.4) holds for this union. But (2.4), on account of its asymptotic nature, is not influenced by the leaving out of a finite number of elements of the set, and therefore it holds for B .

Upper bounds for $\gamma_2(h)$, $\gamma_3(h)$, and $\gamma_4(h)$ can be obtained by means of the construction of bases B for which β_2 , β_3 , and β_4 can be calculated or estimated from above. It is desirable to find upper estimates that are as small as possible, and hence the problem is to construct h -bases that in some sense contain few numbers.

Raikov [24] and Stöhr [30] independently produced the same example of an h -basis B for which $B(n) = O(n^{\frac{1}{h}})$, hence for which β_1 , β_2 , β_3 , and β_4 are finite. Stöhr [29] later showed that for this basis $\beta_3 = \beta_4 = \alpha$, where

$$(2.16) \quad \alpha = \alpha(h) = \max_{t=1,2,\dots,h} (h+t) \sqrt[h]{\frac{1-2^{-h}}{2^{t-1}}}.$$

We shall not prove this here. It follows that

$$(2.17) \quad \gamma_3(h) \leq \gamma_4(h) \leq \alpha.$$

The quantity α can be closely estimated from above by

$$\alpha < \frac{2h}{e \log 2} \sqrt[h]{2} \sqrt[h]{1-2^{-h}}.$$

This basis is constructed as follows: First let an integer $g > 1$ be chosen. Then determine h sets $A^{(j)}$ ($j = 1, 2, \dots, h$) of non-negative integers not exceeding $g-1$ such that every number c in the interval $[0, g-1]$ can be written in the form

$$(2.18) \quad c = \sum_{j=1}^h a^{(j)} \quad (a^{(j)} \in A^{(j)}).$$

Then let $B^{(j)}$ be the set of all numbers

$$(2.19) \quad b^{(j)} = \sum_{i=0}^r a_i^{(j)} g^i \quad (a_i^{(j)} \in A^{(j)})$$

with arbitrarily large r , thus the set of all numbers that can be written in the number system to the base g using numerals only from $A^{(j)}$. Now let B be the union of the h sets $B^{(j)}$.

This set B is an h -basis, for let p be a non-negative

integer and let $p = \sum_{i=0}^r c_i g^i$ be its representation in the

number system to the base g . By (2.18) we can write every c_i in the form $c_i = \sum_{j=1}^h a_i^{(j)}$. Then

$$p = \sum_{j=1}^h \sum_{i=0}^r a_i^{(j)} g^i = \sum_{j=1}^h b^{(j)},$$

and we have p written as the sum of h summands from B .

This h -basis B does not in general satisfy the condition $B(n) = O\left(n^{\frac{1}{h}}\right)$, and certain restrictions must be placed on the sets $A^{(j)}$ in order for it to do so. It is sufficient that all the $A^{(j)}$ contain equally many, say t , numbers, and that $g = t^h$. To show this, we define the $A^{(j)}$ as follows:

$$A^{(j)} = \left\{ 0, t^{j-1}, 2t^{j-1}, \dots, (t-1)t^{j-1} \right\}.$$

The h sets $B^{(j)}$ have the common element zero, among possible others, and hence

$$(2.20) \quad B(n) \leq \sum_{j=1}^h B^{(j)}_n - h + 1.$$

For $n > 0$, let s be the integer such that

$$t^{hs} \leq n \leq t^{h(s+1)} - 1.$$

Then

$$\frac{B(n)}{h\sqrt[n]{n}} \leq \frac{B(t^{h(s+1)} - 1)}{t^s} \leq \frac{h t^{s+1} - h + 1}{t^s} < t h,$$

where the second inequality is found by noting that to form the

elements of $B^{(j)}$ below $t^{h(s+1)} - 1 = g^{s+1} - 1$ we use t coefficients with each of $1, g, g^2, \dots, g^s$ in the sums (2.19). Hence $B(n) = O\left(n^{\frac{1}{h}}\right)$.

We can use this construction to find an upper bound for $\gamma_2(h)$. To do this, we put $t = 2$, and then equality holds in (2.20). Hence, for $n = 2^{hs} - 1$, s a positive integer, we have

$$\frac{B(n)}{\sqrt[n]{n}} = \frac{h \cdot 2^s - h + 1}{\sqrt[2^{hs}]{2^{hs} - 1}} < h.$$

Since this holds for infinitely many n , $\beta_2 \leq h$ for this B , and hence $\gamma_2(h) \leq h$.

Chatrovsky [4] also constructed h -bases for which $B(n) = O\left(n^{\frac{1}{h}}\right)$. For his bases, he obtained

$$B(n) < 64h(h-1) M n^{\frac{1}{h}},$$

where M is a large integer. The upper bound for $\gamma_4(h)$ obtained from this is not as good as (2.17).

Summarizing the results for $\gamma_1(h)$, $\gamma_2(h)$, $\gamma_3(h)$, and $\gamma_4(h)$, we have:

$$\gamma_1(h) = h^{\frac{1}{h}},$$

$$\sqrt[h]{h!} \leq \gamma_2(h) \leq h,$$

and

$$\frac{\sqrt[h]{h!}}{\Gamma(1 + \frac{1}{h})} \leq \gamma_3(h) \leq \gamma_4(h) \leq \alpha,$$

where α is defined by (2.16). The inequalities obtained for $\gamma_2(h)$ correspond to the results for $k_h(n)$ in chapter I.

In connection with the function $k_h(n)$, we discuss briefly the four quantities

$$(2.21) \quad \inf_{n=1,2,\dots} \frac{k_h(n) - 1}{\sqrt[n]{n}} \leq \lim_{n \rightarrow \infty} \inf \frac{k_h(n)}{\sqrt[n]{n}} \\ \leq \lim_{n \rightarrow \infty} \sup \frac{k_h(n)}{\sqrt[n]{n}} \leq \sup_{n=1,2,\dots} \frac{k_h(n) - 1}{\sqrt[n]{n}}$$

From (1.38),

$$(2.22) \quad \frac{k_h^h}{h^h} < n_h(k),$$

whence the quantities (2.21) are finite. We show that the first of them is $\gamma_1(h)$. First we note the following two points: Let n be given and let B run through all h -bases. Then

$$(2.23) \quad \min_B B(n) = k_h(n) - 1,$$

since from every h -basis B there results an h -basis for n by omitting from B all numbers greater than n , and every h -basis for n becomes an h -basis B by uniting with it all integers greater than n . It follows that

$$(2.24) \quad k_h(n) \leq B(n) + 1$$

for every h -basis B . Now, since $\gamma_1(h) \leq \frac{B(n)}{\sqrt[n]{n}}$ for all n

and B , it follows that $\gamma_1(h) \leq \frac{k_h(n) - 1}{\sqrt[n]{n}}$ for all n , whence

$$\gamma_1(h) \leq \inf_{n=1,2,\dots} \frac{k_h(n) - 1}{\sqrt[n]{n}}. \text{ But by (2.24),}$$

$$\inf_{n=1,2,\dots} \frac{k_h(n) - 1}{\sqrt[n]{n}} \leq \inf_{n=1,2,\dots} \frac{B(n)}{\sqrt[n]{n}} \text{ for all } B. \text{ Hence}$$

$$\inf_{n=1,2,\dots} \frac{k_h(n) - 1}{\sqrt[n]{n}} \leq \inf_B \inf_{n=1,2,\dots} \frac{B(n)}{\sqrt[n]{n}} = \gamma_1(h).$$

No explicit expression is known for any of the remaining three quantities (2.21). By means of basis construction, Stöhr [31] shows that

$$\lim_{n \rightarrow \infty} \inf \frac{k_h(n)}{\sqrt[n]{n}} = \gamma_2(h).$$

From (2.24) it follows that

$$\lim_{n \rightarrow \infty} \sup \frac{k_h(n)}{\sqrt[n]{n}} \leq \gamma_3(h) \text{ and } \sup_{n=1,2,\dots} \frac{k_h(n) - 1}{\sqrt[n]{n}} \leq \gamma_4(h);$$

equality has not been proved in these cases.

From Chapter I we have $k_h(n) < h \sqrt[n]{n}$ for $h \geq 2$ and for all n . Hence

$$\lim_{n \rightarrow \infty} \sup \frac{k_h(n)}{\sqrt[n]{n}} \leq h.$$

This is better than the upper estimate (2.17) for $\gamma_3(h)$.

As remarked earlier, the problem of finding good upper estimates for $\gamma_2(h)$, $\gamma_3(h)$, and $\gamma_4(h)$ leads to the search for

bases that are in some sense minimal, that is, bases for which the counting function $B(n)$ is small in some sense. The idea of a minimal basis, while quite clear in connection with bases for an integer n , is not clear when attempts are made to apply it to bases for the integers. Several definitions have been given, most of which require the counting function $B(n)$ of the kind of minimal basis being defined to be less than the counting function of any other basis for certain values of n (for example, for all $n > N$, or for infinitely many n). Stöhr [32] suggests that the following notion might be a substitute for that of a minimal basis: If possible, one would construct an h -basis B such that $\beta_3 = \gamma_3(h)$. In case such a basis does not exist, one constructs instead an infinite sequence $B^{(1)}, B^{(2)}, \dots$ of h -bases such that the sequence $\beta_3^{(1)}, \beta_3^{(2)}, \dots$ tends towards $\gamma_3(h)$.

7. A theorem of Cassels

We briefly discuss here a result of Cassels [3].

Let $b_0 = 1 < b_1 = 1 < b_2 < b_3 < \dots$ denote the elements of an h -basis B ordered according to size. Cassels proved the following theorem:

For $h = 2, 3, \dots$ there exists an h -basis B such that

$$(2.25) \quad \lim_{n \rightarrow \infty} \frac{b_n}{n^h} \text{ exists and is positive.}$$

Furthermore, among such h -bases there is one for which

$$(2.26) \quad b_n = \alpha n^h + o(n^{h-1}),$$

where α is positive and independent of n .

Stöhr (see [31], p. 62) stated that it might be possible to construct an h -basis for which $\lim_{n \rightarrow \infty} \frac{B(n)}{\sqrt[n]{n}}$ exists and is positive. He suggested that such a basis might be obtained in the form of a set of numbers $[f(n)]$ ($n = 0, 1, 2, \dots$) where $f(n)$ is a function for which $\lim_{n \rightarrow \infty} \frac{f(n)}{n^h}$ exists and is positive, and which for almost all n satisfies $[f(n+1)] > [f(n)]$. For example, perhaps $f(n) = \gamma n^h$, where γ is a suitable positive real number, would serve the purpose, or more generally, perhaps a polynomial of degree h in n would serve for $f(n)$. Stöhr mentioned that he was not sure whether, for $h \geq 2$, such a set could be an h -basis. However, Cassels first proved his theorem shortly before Stöhr's paper was written, but he did not publish the result at that time. While Cassels, with this theorem, very nearly meets Stöhr's demands, he did not, in his proof, construct bases satisfying (2.25) and (2.26), but rather only proved that such bases exist.

Cassels divided his theorem into two parts, one part for $h > 2$ and one for $h = 2$. For $h = 2$ he proved the existence of bases A , B , and C such that

$$(2.27) \quad \lim_{n \rightarrow \infty} \inf \frac{a_{n+1} - a_n}{n} = \frac{2}{11 + 5^{\frac{3}{2}}} \approx \frac{1}{11},$$

$$(2.28) \quad \lim_{n \rightarrow \infty} \inf \frac{b_n}{n^2} = \frac{8}{71 + 17^{\frac{3}{2}}} \doteq \frac{3}{53} ,$$

and

$$(2.29) \quad \lim_{n \rightarrow \infty} \frac{c_n}{n^2} = \frac{1}{27} .$$

For $h > 2$, he found no specific value for the limit in (2.25).

The limits (2.28) and (2.29) should be compared with the inequality

$$(2.30) \quad \lim_{n \rightarrow \infty} \inf \frac{b_n}{n^2} \leq \frac{\pi}{8}$$

which holds for every 2-basis B . This inequality is obtained as

follows: Let $\varepsilon > 0$ be given, and let $\beta = \lim_{n \rightarrow \infty} \inf \frac{b_n}{n^2}$.

Then, for sufficiently large m ,

$$(1 + \varepsilon \beta) \frac{b_m}{m^2} > \beta .$$

Hence, from

$$b_m + b_n \leq x$$

there follows

$$(1 + \varepsilon \beta) x \geq (1 + \varepsilon \beta)(b_m + b_n) > (m^2 + n^2)\beta ,$$

or

$$(2.31) \quad m^2 + n^2 < \left(\frac{1}{\beta} + \varepsilon \right) x$$

if x is sufficiently large. The number of solutions of (2.31),

for $m \leq n$, is

$$\frac{\pi}{8} \left(\frac{1}{\beta} + \varepsilon \right) x + O(\sqrt{x}) ,$$

by the argument involving the lattice points in a sector with central angle $\frac{\pi}{4}$ in a circle of radius $\sqrt{(\frac{1}{\beta} + \varepsilon) x}$. Since B is a 2-basis, the number of solutions of $b_m + b_n \leq x$ is at least x , and hence

$$x \leq \frac{\pi}{8} \left(\frac{1}{\beta} + \varepsilon \right) x + o(\sqrt{x}) .$$

The inequality (2.30) follows.

CHAPTER III

DIFFERENCE BASES

8. Introduction

In this chapter we discuss some results of Rédei and Rényi [25], and some improvements on and extensions of these results by Leech and Hazelgrove [18], [19]. The results concern the representation of each of the integers $1, 2, \dots, n$ as the difference between some two elements of a set of integers.

A set A of integers $a_1, \dots, a_k$ is called a difference basis for n if every integer m in the interval $0 < m \leq n$ can be represented in the form $m = a_i - a_j$. Since the sets A and $A + \{d\}$, where d is an integer, have the same set of differences, it will not affect the difference basis property of A if we assume that its elements a_i are all non-negative. The minimum value of k for given n is denoted by $k(n)$. $A : a_1, \dots, a_\ell$ is called a restricted difference basis for n if $0 \leq a_i \leq n$ for $a_i \in A$. The minimum value of ℓ for given n is denoted by $\ell(n)$. Clearly a restricted difference basis for n must contain both 0 and n . When the meaning is clear we may write simply "basis" instead of "difference basis for n ". We shall refer to the bases of the previous chapters as addition bases.

For a difference basis for n with k elements we have $\binom{k}{2} \geq n$, whence $k > \sqrt{2n}$. From Rohrbach [26] we obtain the following restricted difference basis of $\ell = x + y$ elements for the integer $yx + y - 1$:

$$0, 1, 2, \dots, x-1, x, 2x+1, 3x+2, \dots, yx + y-1 .$$

However, we can make a slight modification to obtain

$$(3.1) \quad 0, 1, 2, \dots, x-1, x, 2x+2, 3x+3, \dots, yx + y ,$$

a restricted difference basis for $yx + y$ with $\ell = x + y$ elements. From this it can be shown that for given n , there exists a restricted difference basis of ℓ elements such that $\ell < \sqrt{4n + 1}$. Brauer [2] found a slightly improved basis for which $\ell < 2 \sqrt{n + \frac{52}{9}} - \frac{4}{3}$, whence $\ell < 2 \sqrt{n}$ if $n > 16$. We therefore have, for $n > 16$,

$$(3.2) \quad \sqrt{2n} < k(n) \leq \ell(n) < 2 \sqrt{n} ,$$

corresponding to the inequalities (1.4) for addition bases of order 2 for n . Here, however, improvements have been made in both the upper and the lower estimates, for large enough n . This is what Rédei, Rényi, Leech, and Hazelgrove have done. Moreover, they have obtained a lower estimate considerably better than that found for addition 2-bases (see (1.6)).

It is interesting to note that while $\lim_{n \rightarrow \infty} \frac{k(n)}{\sqrt{n}}$ and $\lim_{n \rightarrow \infty} \frac{\ell(n)}{\sqrt{n}}$ have been shown to exist (see below), the corresponding result for addition h -bases, namely $\lim_{n \rightarrow \infty} \frac{k_h(n)}{\sqrt[n]{n}}$

exists, has not been proved for $h > 1$. (See the discussion of $k_h(n)$ in the latter part of § 6.)

9. On the ratios $\frac{k(n)}{\sqrt{n}}$ and $\frac{\ell(n)}{\sqrt{n}}$.

Rédei and Rényi showed that

$$(3.3) \quad \lim_{n \rightarrow \infty} \frac{k(n)}{\sqrt{n}} \text{ exists and is } \inf_{n=1,2,\dots} \frac{k(n)}{\sqrt{n}}$$

and

$$(3.4) \quad \sqrt{2.424} < \left(2 + \frac{4}{3\pi}\right)^{\frac{1}{2}} \leq \lim_{n \rightarrow \infty} \frac{k(n)}{\sqrt{n}} \leq \left(\frac{8}{3}\right)^{\frac{1}{2}} .$$

Leech [18] made slight improvements on the bounds in (3.4), obtaining

$$(3.5) \quad \sqrt{2.434} \leq \lim_{n \rightarrow \infty} \frac{k(n)}{\sqrt{n}} \leq \sqrt{2.6647} .$$

The estimates in (3.5) are found by extending slightly the arguments of Rédei and Rényi.

Erdős and Gal [13] stated that (3.3) and (3.4) hold with $k(n)$ replaced by $\ell(n)$. However, Leech found their work to be invalid, and he amended their proof to obtain

$$(3.6) \quad \lim_{n \rightarrow \infty} \frac{\ell(n)}{\sqrt{n}} \text{ exists and is } \inf_{n=1,2,\dots} \frac{\ell(n) + \lambda}{\sqrt{n+1}} \text{ for } \lambda \geq 2$$

and

$$(3.7) \quad \sqrt{2.434} \leq \lim_{n \rightarrow \infty} \frac{\ell(n)}{\sqrt{n}} \leq \sqrt{3.3483} .$$

The left hand inequality in (3.7) follows from (3.5). Then Leech and Hazelgrove [19] proved (3.6) for $\lambda \geq 1.68662 \dots$,

and obtained the improved estimate $\sqrt{3.3342\dots}$ for the right hand side of (3.7).

We shall here prove (3.3) and (3.5), the main part of the proof of the latter being the proof of (3.4).

We proceed to a proof of (3.3).

Let $r \geq 1$ be a given integer, and let $\beta > 0$ be given. Let $\theta > 0$ be a real number such that $\theta \frac{k(r)}{\sqrt{r}} < \frac{\beta}{2}$. Then there exists an integer $N = N(r, \beta)$ such that for $n > N$, $\frac{k(r)}{\sqrt{n}} < \frac{\beta}{2}$

and there is a prime q in the interval $\sqrt{\frac{n}{r}} < q < (1 + \theta)\sqrt{\frac{n}{r}}$.

This last is a consequence of the prime number theorem; it is

easily shown that there is always a prime p satisfying

$x < p < (1 + \varepsilon) x$ when $x > x_0(\varepsilon)$ (see Hardy and Wright [15],

p. 371). Now, for t a power of a prime, Singer [28] proved

that there exist $t + 1$ integers $b_1, b_2, \dots, b_{t+1}$ such that

the differences $b_g - b_h$ form a complete residue system modulo

$t^2 + t + 1$; he called such a set of integers a perfect

difference set of order $t + 1$. Let $m = q^2 + q + 1$. We choose a

perfect difference set of order $q + 1$:

$$(3.8) \quad 0 = b_1 < b_2 < \dots < b_{q+1} < m.$$

Then, given any integer s such that $0 \leq s \leq m-1$, there exist

two integers b_g and b_h in the set such that either $s = b_g - b_h$

or $s - m = b_g - b_h$.

Now let

$$(3.9) \quad A : 0 = a_1 < a_2 < \dots < a_{k(r)}$$

be a difference basis for r having the minimum number $k(r)$ of elements. Then the set of integers

$$(3.10) \quad a_i m + b_g \quad (i = 1, 2, \dots, k(r) ; \quad g = 1, 2, \dots, q+1)$$

is a difference basis for mr . To show this, let $s = s_1 m + s_2$ be an integer in the interval $0 \leq s \leq m r$, where $0 \leq s_1 \leq r - 1$, $0 \leq s_2 \leq m - 1$. If s_2 can be written $s_2 = b_g - b_h$, then we choose a_i and a_j so that $s_1 = a_i - a_j$, whence $s = (a_i m + b_g) - (a_j m + b_h)$. If s_2 is such that $s_2 - m = b_g - b_h$, then we choose a_i and a_j so that $s_1 + 1 = a_i - a_j$, whence $s = (a_i m + b_g) - (a_j m + b_h)$. Finally, $m r = (a_i m + b_g) - (a_j m + b_g)$ if $a_i - a_j = r$, as must be the case for some pair a_i, a_j .

It follows that $k(m r) \leq (q + 1) k(r)$. Since $\sqrt{\frac{n}{r}} < q$, $n < m r$. Therefore

$$k(n) \leq (q+1) k(r) < \left\{ (1 + \theta) \sqrt{\frac{n}{r}} + 1 \right\} k(r).$$

Hence, for any integer r , any $\beta > 0$, and $n > N(r, \beta)$, we have

$$\frac{k(n)}{\sqrt{n}} < \left(\frac{1 + \theta}{\sqrt{r}} + \frac{1}{\sqrt{n}} \right) k(r) < \frac{k(r)}{\sqrt{r}} + \beta.$$

Therefore $\frac{k(n)}{\sqrt{n}}$ converges to its infimum, proving (3.3).

We find the right hand inequality in (3.4) by noting that $\{0, 1, 4, 6\}$ is a difference basis for 6, whence

$$\frac{k(6)}{\sqrt{6}} = \sqrt{\frac{8}{3}}. \quad \text{Leech obtained the improvement in (3.5) by}$$

noting that no integer s in the interval $b_{q+1} < s < m$ can be written in the form $b_g - b_h$, and that hence the integers $-1, -2, \dots, -(m - b_{q+1} - 1)$ can be written in the form $b_g - b_h$, or the integers $1, 2, \dots, m - b_{q+1} - 1$ in the form $b_h - b_g$. Choosing a_i and a_j so that $a_i - a_j = r$, we can express the integers

$$mr + 1, mr + 2, \dots, mr + m - b_{q+1} - 1$$

as differences between pairs of integers $(a_i m + b_h)$, $(a_j m + b_g)$ of the set (3.10). Hence the set (3.10) is a difference basis for $R = m r + m - b_{q+1} - 1$. Hence

$$\begin{aligned} \frac{k^2(R)}{R} &\leq \frac{(q+1)^2 k^2(r)}{mr + m - b_{q+1} - 1} \\ &= \frac{k^2(r)}{r} \frac{q^2 + 2q + 1}{q^2 + q + 1 + \frac{m - b_{q+1} - 1}{r}}, \end{aligned}$$

and therefore $\frac{k^2(R)}{R} < \frac{k^2(r)}{r}$ if $m - b_{q+1} - 1 > r q$. Leech evaluated $\max(m - b_{q+1} - 1)$ for various values of q and found that ^{for} $q = 32$, $\max(m - b_{q+1} - 1) = 197 = 6q + 5$, the perfect difference set for this being

0	22	38	47	91	108	123	136	141	229	256
263	293	319	329	358	360	400	406	505	516	524
559	573	633	684	685	705	708	763	767	847	859

With this set for the b_h , and $A = \{0, 1, 4, 6\}$, he obtained a difference basis of $4 \times 33 = 132$ elements for $R = 6539$, whence

$$\frac{k^2(R)}{R} \leq \frac{17424}{6539} = 2.6646 \dots$$

The right hand inequality in (3.5) follows.

To prove the left hand inequality in (3.4), let

$A : a_1 < a_2 < \dots < a_k$ be a (not necessarily minimal) difference basis for n . For t an integer, let $f(t)$ be the number of representations of t in the form $a_r - a_s$; f will of course count the number of representations of $t = 0$ and of integers $t < 0$. Then

$$\begin{aligned} & \left(\sum_{r=1}^k \cos a_r x \right)^2 + \left(\sum_{s=1}^k \sin a_s x \right)^2 \\ &= \sum_{r=1}^k \sum_{s=1}^k \cos a_r x \cos a_s x + \sum_{r=1}^k \sum_{s=1}^k \sin a_r x \sin a_s x \\ &= \sum_{r=1}^k \sum_{s=1}^k \cos(a_r - a_s)x \\ (3.11) \quad &= \sum_t f(t) \cos t x . \end{aligned}$$

Since A is a difference basis for n , $f(t) > 0$ for $t = 0, \pm 1, \pm 2, \dots, \pm n$, and therefore $\delta(t) \geq 0$ in the following equation:

$$(3.12) \quad \sum_t f(t) \cos tx = f(0) + 2 \sum_{s=1}^n \cos sx + \sum_t \delta(t) \cos tx .$$

Of course, $f(0) = k$, and putting $x = 0$ here yields

$$k^2 = k + 2n + \sum_t \delta(t) ,$$

since $\sum_t f(t) = k^2$ by (3.11). The lower estimate in (3.2) follows directly. To improve on (3.2), we must show that $\sum_t \delta(t)$ is large; in fact, we show that it is of the order of n . Now,

$$(3.13) \quad \sum_t \delta(t) \geq \sum_t \delta(t) \cos tx ,$$

and the right hand side here is large for a value of x that makes $2 \sum_{s=1}^n \cos sx$ negative and large, because by (3.11), $\sum_t f(t) \cos tx \geq 0$. By (3.12) and (3.13),

$$\begin{aligned} \sum_t \delta(t) &\geq \sum_t f(t) \cos tx - k - 2 \sum_{s=1}^n \cos sx \\ &\geq -k - 2 \sum_{s=1}^n \cos sx , \end{aligned}$$

and hence

$$(3.14) \quad k^2 \geq 2n - 2 \sum_{s=1}^n \cos sx .$$

Using, with Rédei and Rényi, $\frac{3\pi}{2n+1}$ as a value of x that makes

$$2 \sum_{s=1}^n \cos sx = \frac{\sin \frac{2n+1}{2} x}{\sin \frac{x}{2}} - 1$$

negative and large, we obtain, from (3.14),

$$(3.15) \quad k^2 \geq 2n + \frac{1}{\sin \frac{3\pi}{4n+2}} + 1 \geq 2n + \frac{4n+2}{3\pi} + 1 .$$

Hence

$$\frac{k^2}{n} > 2 + \frac{4}{3\pi},$$

and the left hand inequality in (3.4) follows since $k(n)$ is a possible value of k here.

This result can be improved by finding a value of x that makes $\frac{\sin \frac{2n+1}{2} x}{\sin \frac{x}{2}}$ less than the value found for it above.

We consider values of x that are of the order of $\frac{1}{n}$, like that used above. For large n , x will be small, whence $\sin nx$ and $\frac{x}{2}$ are close approximations to $\sin \frac{2n+1}{2} x$ and $\sin \frac{x}{2}$.

Using these approximations, we obtain, from (3.14),

$$k^2 \geq 2n - \frac{2 \sin nx}{x} = 2n(1 - \frac{\sin nx}{nx}).$$

We put $\theta = nx$; then $\theta = \frac{3\pi}{2}$ gives the Rédei and Rényi result. However, $\frac{\sin \theta}{\theta}$ is a minimum at the point θ in the interval

$(\pi, \frac{3\pi}{2})$ at which $\theta = \tan \theta$. From tables we find this value of θ to be 4.491 ..., whence the left hand inequality in (3.5) is obtained.

Brauer's main result in the paper [2], referred to above, is that $\ell(30) = 10$. His method of proof is applicable to any given value of n , although the details are different for different values of n , and for large n the amount of work necessary is correspondingly large. (One might compare our computation of $n_2(7)$ and $n_2(8)$ in §3 with Brauer's computation of $\ell(30)$.) Two restricted difference bases for 30 with 10 elements are

$\{0, 1, 2, 3, 4, 10, 15, 20, 25, 30\}$ and $\{0, 1, 2, 3, 4, 5, 12, 18, 24, 30\}$, these sets being obtained from (3.1) by putting $x = 4$, $y = 6$

for the first and $x = y = 5$ for the second. Brauer's paper is interesting partly since it describes one of the few applications of additive number theory. A variable resistance was to be constructed having a number of fixed contact points such that each integral resistance from 1 to 30 ohms could be obtained by connecting some two of the contact points, and it was of interest to know the smallest number of contact points necessary. Brauer devoted part of his paper to a discussion of more general problems on difference bases, and constructed the basis mentioned in § 8. He also stated that it is very likely that the true value of $n(\ell)$, where $n(\ell)$ is the largest integer for which a difference basis of ℓ elements exists, is $\frac{\ell^2}{4} + o(\ell)$. This corresponds to Rohrbach's conjecture (1.5) for addition 2-bases, but it is false on account of (3.5) and (3.7).

In closing this chapter we discuss briefly difference bases for all the integers, analogous to the addition bases for the non-negative integers discussed in Chapter II. Stöhr [31] defines a universal difference basis as a set A of integers $a_0, a_1, a_2, \dots$ such that any integer x is representable in the form $a_i - a_j$. The problem of specifying a universal difference basis A of non-negative integers such that $A(n)$ is small in some sense is not very interesting, since if $c_1, c_2, c_3, \dots$ is a sequence of non-negative integers, and A is the set $\{c_1, c_1+1, c_2, c_2+2, c_3, c_3+3, \dots\}$, then A is a universal difference basis with a counting function that can be made to tend to ∞ arbitrarily slowly through the choice of a

sufficiently rapidly increasing sequence $\{c_i\}$. In place of a counting function Stöhr defines a function $g(n)$ for a universal difference basis A as follows: let $i(x)$ be the smallest number such that $x = a_i - a_j$, with $i, j \leq i(x)$, is solvable; for every integer $n \geq 0$ let $g(n) = \max_{|x| \leq n} i(x)$. Thus $a_0, a_1, \dots, a_{g(n)}$ form a difference basis for n , and it follows that $k(n) \leq g(n) + 1$. On the other hand, $a_0, a_1, \dots, a_{k(n)-1}$ form a difference basis for n which can be complemented to form a universal difference basis, and hence for given n ,

$$\min g(n) = k(n) - 1,$$

where the minimum is over all universal difference bases. The analogous statement for addition bases is (2.23). It follows from this, as well as from the fact that $\sqrt{n} \leq \binom{g(n) + 1}{2}$, that $\sqrt{n} = O(g(n))$. On the other hand, Stöhr gives a method of constructing universal difference bases for which $g(n) = O(\sqrt{n})$.

CHAPTER IV

SOME RELATED PROBLEMS

10. Introduction

We discuss here problems concerning the sums of pairs of integers; in some problems the integers in a pair are both taken from the same sequence, and in others they come from two different sequences. These sequences are not necessarily 2-bases. The problems to be dealt with are discussed briefly, along with other problems, by Erdős in [9] and [10].

In §11 we consider some results and conjectures of Erdős, Turán, and Fuchs [14], [12] concerning the number of times n can be represented in the form $a_i + a_j$ where a_i and a_j are elements of the same sequence. In §12 we prove a result of Lorentz [20] concerning sequences A and B such that $A + B$ contains nearly all (i.e., all but a finite number of) positive integers. In §13 we prove results of Erdős and Turán [14], [8] on sequences of integers whose sums in pairs are all different, and end with a brief discussion of a generalization of these results to results with sums r at a time, obtained by Bose and Chowla [1].

11. Some results of Erdős, Turán, and Fuchs

In this section we discuss some results and conjectures of Erdős, Turán, and Fuchs [14], [12].

We use the letter A to denote a sequence of non-negative

integers $a_1 < a_2 < \dots$. We denote by $f(n)$ the number of representations of n in the form $a_i + a_j$. Erdős and Turán considered the question: Is it possible, for some set A , that $f(n)$ is constant for all sufficiently large n ?

The question in this form is not sufficiently precise, since the multiplicities to be taken in a representation have not been specified. The number $f(n)$ can be interpreted in three different ways. We can count a representation $a_i + a_j$:

- (i) twice if $i \neq j$ and once if $i = j$;
- (ii) once if $i \neq j$ and once if $i = j$;
- (iii) once if $i \neq j$ and not at all if $i = j$.

Erdős and Turán considered only case (i) and proved a negative answer. Dirac [6] , however, pointed out that the question in case (i) is trivial, since if $n = a_i + a_i$, $f(n)$ is odd, and if n cannot be represented in this way, $f(n)$ is even. Dirac gave two other possible definitions of $f(n)$, which are essentially (ii) and (iii) above.

If we put $g(z) = \sum_{k=1}^{\infty} z^{a_k}$, then the generating functions $\sum_{n=0}^{\infty} f(n) z^n$ in the three cases are (i) $g^2(z)$, (ii) $\frac{1}{2} (g^2(z) + g(z^2))$, and (iii) $\frac{1}{2} (g^2(z) - g(z^2))$. (Dirac's definitions of $f(n)$ would eliminate the factor $\frac{1}{2}$ in (ii) and (iii).) In case (ii), Dirac proved a negative answer to Erdős and Turán's question. The argument here is that

$f(n) = f(n_0)$ for all $n \geq n_0$ is equivalent to

$$\frac{g^2(z) + g(z^2)}{2} = \frac{f(n_0)}{1-z} + P(z),$$

where $P(z)$ is a polynomial in z of degree less than n_0 . Now, if $z \rightarrow -1$ from above, the right hand side remains bounded, but the left hand side tends to infinity since both terms in the numerator are positive and the second term tends to infinity.

Newman, in a written communication to Erdős, proved the same result independently, but neither Dirac nor Newman found an answer for case (iii).

Finally, Erdős and Fuchs [12] proved in all three cases that if $c > 0$, or $c = 0$ and $a_j < M j^2$, then

$$\lim_{n \rightarrow \infty} \sup \frac{1}{n} \sum_{k=0}^n (f(k) - c)^2 > 0,$$

thus answering the question completely. Erdős and Fuchs proved also the Erdős-Turán conjecture that it is impossible that

$$(4.1) \quad \sum_{k=0}^n f(k) = c n + o(1),$$

where c is a constant. In fact they proved, for all three interpretations of $f(k)$, that if $c > 0$,

$$(4.2) \quad \sum_{k=0}^n f(k) = c n + o\left(\frac{n^{\frac{1}{4}}}{\sqrt{\log n}}\right)$$

cannot hold. Note that (4.1) clearly cannot hold if $c = 0$,

but that $c \neq 0$ is necessary if (4.2) is to be false, for if $c = 0$, (4.2) could hold if $a_k \rightarrow \infty$ sufficiently rapidly.

This second result of Erdős and Fuchs compares well with the result of Hardy and Landau for the sequence of squares ($a_k = k^2$), namely the result that

$$\sum_{k=0}^n f(k) = \pi n + o \left\{ (n \log n)^{\frac{1}{4}} \right\}$$

does not hold. While this is stronger than the statement that (4.2) is false, Erdős and Fuchs's result holds for all sequences.

Erdős and Fuchs considered it likely that there exists a sequence A for which $\sum_{k=0}^n f(k) = c n + O(n^{\frac{1}{4}})$, but this has not been proved.

Both of the above results of Erdős and Fuchs imply that $f(k)$ is not constant from some value of k onward for any sequence A. But they imply more than this. For example, we prove that $f(k)$ is not periodic from some point on for any sequence A: Suppose that $f(k)$ is periodic for $k > m$. Then for $k > m$ and some integer t , $f(k)$ will take successively the values $b_1, b_2, \dots, b_t, b_1, b_2, \dots, b_t, \dots$, say. From $k = m+1$ to $k = n$, $f(k) = b_i$ occurs either

$$\left[\frac{n-m}{t} \right] \text{ or } \left[\frac{n-m}{t} \right] + 1 \text{ times. Hence}$$

$$\begin{aligned} \sum_{k=0}^n f(k) &= \sum_{k=0}^m f(k) + \left[\frac{n-m}{t} \right] (b_1 + b_2 + \dots + b_t) + O(1) \\ &= c n + O(1). \end{aligned}$$

The result follows since (4.1) is false.

Another conjecture of Erdős and Turán was that if $f(k) > 0$ for $k > k_0$ (i.e. if A is an asymptotic 2-basis), then $\lim_{k \rightarrow \infty} \sup f(k) = \infty$. This conjecture has not been proved. On the other hand, Sidon, in an oral communication to Erdős, asked whether there exists a sequence satisfying the two conditions $f(n) > 0$ for all sufficiently large n and $\lim_{n \rightarrow \infty} \frac{f(n)}{n^\epsilon} = 0$ for all $\epsilon > 0$. Erdős [7] proved the existence of such a sequence; in fact he proved the existence of a sequence satisfying

$$0 < f(n) < c \log n$$

for $n > n_0$, c a constant. He did not succeed in constructing such a sequence, however.

3. A theorem of Lorentz

In this section we prove a theorem of Lorentz [20]. We first give the following definition: Two sequences A and B of non-negative integers are called complementary to each other if there exists a non-negative integer M such that $A + B$ contains all integers greater than M .

Lorentz proved the following result:

THEOREM.

Let A be a sequence of non-negative integers. Then there exists a complementary set B such that

$$(4.3) \quad B(n) \leq c \sum_{k=1}^n \frac{\log A(k)}{A(k)} ;$$

the terms of the sum with $A(k) = 0$ or 1 are to be replaced by one.

Before proving this theorem, we prove the following lemma:

LEMMA.

Let A be a given sequence of non-negative integers. Let i and j be non-negative integers such that $i \leq j$. Then we can choose integers b in the interval $i \leq b < 2j$ in such a way that the sums $a+b$, $a \in A$, fill the interval $j < a + b \leq 2j$, and the number K of these b 's satisfies

$$(4.4) \quad K \leq c_1 \frac{j \log A(j-i+1)}{A(j-i+1)} \quad . \quad ^1)$$

If $A(j-i+1) = 0$ or 1 , we can replace the right hand side here by $c_1 j$. (c_1 , and later $c_2, c_3, \dots$, denote constants.)

PROOF:

For our first b we choose an integer b_1 in the interval $[i, 2j)$ in such a way that the subset of $A + \{b_1\}$ that is contained in $(j, 2j]$ has the greatest possible number $S (\leq j)$ of elements. Then we choose b_2 in $[i, 2j)$ in such a way that $A + \{b_2\}$ contains the greatest possible number of integers in $(j, 2j]$ that do not belong to $A + \{b_1\}$, and so on.

¹⁾ There would be some difficulty here if the least element of A , say t , exceeded $j+1$. In this case we shall count as b 's the integers in the open interval (j, t) if $j+1 < t \leq 2j$, or the integers in $(j, 2j)$ if $t > 2j$. More simply, we could obviate the difficulty by requiring that A contain zero, but we wish to avoid such a restriction.

To each non-negative integer s ($\leq S$) there corresponds a certain number of b 's such that $A + \{b\}$ contains exactly s new points in $(j, 2j]$. Let K_s be the number of these translations $A + \{b\}$, $i \leq b < 2j$. We shall say that these b 's correspond to the value s .

After all the elements b corresponding to the values $S, S-1, \dots, s+1$ are chosen, there will remain a set R of integers in $(j, 2j]$ that are not covered (i.e., that do not belong to any of the sets $A + \{b\}$). Let $r_1 < r_2 < \dots < r_k$ ($k = k_s$) be the elements of R . If s is zero, R is empty and hence $k_0 = 0$. For $s = 1, 2, \dots$, it is easily seen that $k_{s-1} = k_s - s K_s$, or

$$(4.5) \quad K_s = \frac{k_s - k_{s-1}}{s}.$$

We now find an upper bound for k_s , which we use together with (4.5) to derive (4.4). Consider the number of times the points of R are covered by the translations $A + \{i\}$, $A + \{i+1\}$, $\dots$, $A + \{2j-1\}$. Each translation covers at most s points of R , and therefore the number of coverings does not exceed $(2j-1)s \leq 2js$. But a point r_m in R is covered exactly $A(r_m - i)$ times. Hence

$$A(r_1 - i) + A(r_2 - i) + \dots + A(r_k - i) \leq 2js,$$

and therefore $k A(j - i + 1) \leq 2js$, since $r_m \geq j + 1$. Hence

$$(4.6) \quad k_s \leq \frac{2js}{A(j-i+1)}.$$

Let s_0 be an integer greater than 1. The number of b 's corresponding to values $s < s_0$ is $\sum_{s=1}^{s_0-1} K_s$, and the number corresponding to values $s \geq s_0$ does not exceed $\frac{j}{s_0}$, since each choice of a b leads to the covering of at least s_0 new points in $(j, 2j]$. Hence

$$K \leq \sum_{s=1}^{s_0-1} K_s + \frac{j}{s_0},$$

whence, by (4.5) and (4.6),

$$\begin{aligned} K &\leq \sum_{s=1}^{s_0} \frac{k_s - k_{s-1}}{s} + \frac{j}{s_0} \\ &= \sum_{s=1}^{s_0-1} \frac{k_s}{s(s+1)} + \frac{k_{s_0}}{s_0} + \frac{j}{s_0} \\ &\leq \frac{2j}{A(j-i+1)} \sum_{s=1}^{s_0} \frac{1}{s} + \frac{j}{s_0} \\ &\leq \frac{c_2 j \log s_0}{A(j-i+1)} + \frac{j}{s_0}, \end{aligned}$$

since $\log s_0 < \sum_{s=1}^{s_0} \frac{1}{s} < \log s_0 + 1$. We wanted $s_0 > 1$ because of the last step. We consider now the case $A(j-i+1) > 1$; the case $A(j-i+1) = 0$ or 1 is dealt with below. We take

$$s_0 = \left\lceil \frac{A(j-i+1)}{\log A(j-i+1)} \right\rceil; \text{ then } s_0 > 1, \text{ since for } x > 1,$$

$$\frac{x}{\log x} \geq e \text{ and } \left\lceil \frac{x}{\log x} \right\rceil \geq 2. \text{ Writing } A(j-i+1) = a \text{ for}$$

convenience, we have

$$K \leq c_2 j \frac{\log a - \log \log a}{a} + j \frac{\log a}{a - \log a}$$

$$\leq j \frac{\log a}{a} \left(c_2 + \frac{1}{1 - \frac{\log a}{a}} \right).$$

Since $\frac{\log x}{x} \leq \frac{1}{e}$ for any x , we can choose a constant c_1

such that $\frac{\log a}{a} < 1 - \frac{1}{c_1 - c_2}$, and hence

$$K \leq c_1 j \frac{\log a}{a},$$

yielding (4.4) for the case $A(j - i + 1) > 1$. Replacing the right hand side in (4.4) by $c_1 j$ if $A(j - i + 1) = 0$ or 1 is clearly valid since $c_1 > 1$. The lemma therefore holds.

We proceed with the proof of the theorem.

We state the following procedure for constructing B .

For each $m = 1, 2, \dots$ put $j = j(m) = 2^m$, $i = i(m) = 2^{m-1} + 1$, $K = K(m)$, and denote the set of b 's in $(2^{m-1}, 2^{m+1})$, chosen as in the proof of the lemma, by B_m . Then put $B = \cup B_m$. By the lemma,

$$(4.7) \quad K(m) \leq c_3 \frac{2^{m-2} \log A(2^{m-1})}{A(2^{m-1})}.$$

Let n be a positive integer. We denote by $B_m(n)$ the number of elements of B in the interval $(2^{m-1}, 2^{m+1})$ that do not exceed n . Then

$$B(n) \leq \sum_m B_m(n)$$

$$\leq \sum_{2^{m-1} \leq n} K(m),$$

it being necessary to take the last sum over only those m for which $2^{m-1} \leq n$, since $B_m(n) = 0$ for $n \leq 2^{m-1}$. Hence

$$B(n) \leq c_3 \sum_{\substack{m \\ 2^{m-1} \leq n}} 2^{m-2} \frac{\log A(2^{m-1})}{A(2^{m-1})} \quad (\text{by (4.7)})$$

$$\leq c_4 \sum_{\substack{m \\ 2^{m-1} \leq n}} \sum_{2^{m-2} < k \leq 2^{m-1}} \frac{\log A(k)}{A(k)},$$

since $\frac{\log(x+1)}{x+1} < \frac{\log x}{x}$ for $x \geq 3$; the constant is changed from c_3 to c_4 to adjust for the sums $\sum_{2^{m-2} < k \leq 2^{m-1}} \frac{\log A(k)}{A(k)}$

in which $A(k)$ changes from 1 to 2 and from 2 to 3. Only for the values of m involved in these two sums is it possible that

$$2^{m-2} \frac{\log A(2^{m-1})}{A(2^{m-1})} \geq \sum_{2^{m-2} < k \leq 2^{m-1}} \frac{\log A(k)}{A(k)}.$$

When $A(k) = 0$ or 1, $\frac{\log A(k)}{A(k)}$ is replaced by one, a valid procedure because of the lemma. Lorentz's theorem follows.

Erdős, in an oral communication to Lorentz, had conjectured that each sequence A has a complementary sequence B of asymptotic density zero. The truth of this conjecture follows from Lorentz's theorem, for let $\gamma > 0$ be given. Then there exists an integer M such that for $k > M$, $c \frac{\log A(k)}{A(k)} < \gamma$. Hence, for some sequence B complementary to a given sequence A , we have

$$\begin{aligned} \frac{B(n)}{n} &\leq \frac{c \sum_{k=1}^n \frac{\log A(k)}{A(k)}}{n} \\ &< \frac{c \sum_{k=1}^M \frac{\log A(k)}{A(k)} + (n-M) \gamma}{n}, \end{aligned}$$

and this tends to γ as $n \rightarrow \infty$. Hence $\lim_{n \rightarrow \infty} \frac{B(n)}{n} = 0$.

Lorentz's theorem provides answers to many problems with special sequences A . For example, let A be the sequence of primes. Then $A(k) = \pi(k)$, and using Chebyshev's theorem, namely $c_5 \frac{k}{\log k} < \pi(k) < c_6 \frac{k}{\log k}$, we find that the primes have a complementary sequence B such that

$$\begin{aligned} B(n) &\leq c \sum_{k=1}^n \frac{\log \pi(k)}{\pi(k)} \\ &< c \sum_{k=1}^n \frac{(\log c_6 + \log k - \log \log k) \log k}{c_5 k} \\ &< c_7 \sum_{k=1}^n \frac{\log^2 k}{k} \\ &< c_8 \log^3 n. \end{aligned}$$

Erdős [11] improved this to $c_9 \log^2 n$. Again, if A is the sequence of squares, then $A(k) = \lfloor \sqrt{k} \rfloor$, and by Lorentz's theorem there is a complementary sequence B such that $B(n) < c_{10} \sqrt{n} \log n$. Also in [11], Erdős improved on this, showing that there is a complementary sequence B with

$B(n) < c_{11} \sqrt{n}$. His sequence B is the union of the sets of integers in the intervals

$$2^k < b < 2^k + 4 \cdot 2^{\frac{k}{2}}, \quad k = 1, 2, \dots$$

Finally, if A is the sequence of the powers of 2, the theorem shows that there is a complementary sequence B such that $B(n) < \frac{c_{12} n \log \log n}{\log n}$. The conjecture of Erdős [11] that there exists a B such that $B(n) < \frac{c_{13} n}{\log n}$ has not been proved.

13. B_2 sequences

Let $A : a_1 < a_2 < \dots$ be a sequence of positive integers such that the sums $a_i + a_j$ (where $i \leq j$) are all different. Sidon [27] called such a sequence a B_2 sequence. Let n be a given positive integer, and let $A(n)$ be the counting function of A . Now, letting A run through all B_2 sequences, we put

$$F(n) = \max_A A(n) .$$

We can give $F(n)$ the following simple meaning: We define a (finite) B_2 sequence for n as a set of positive integers $a_1 < a_2 < \dots < a_x \leq n$ such that the sums in pairs of the integers are all different. Then $F(n)$ is the maximum value of x ; that is, it is the maximum number of elements that a B_2 sequence for n can have.

Erdős and Turán [14] proved that

$$\frac{1}{\sqrt{2}} \leq \lim_{n \rightarrow \infty} \inf \frac{F(n)}{\sqrt{n}} \leq \lim_{n \rightarrow \infty} \sup \frac{F(n)}{\sqrt{n}} \leq 1 .$$

Then Erdős [8] , using a result of Singer [28] regarding perfect difference sets (see § 9), raised the lower limit here to one. This was proved also by Chowla [5] . Thus

$$(4.8) \quad \lim_{n \rightarrow \infty} \frac{F(n)}{\sqrt{n}} = 1 .$$

We proceed with a proof of (4.8).

Singer's result implies that if t is a prime power, then there exist $t + 1$ positive integers

$$a_1 < a_2 < \dots < a_{t+1} \leq t^2 + t + 1$$

such that the differences $a_i - a_j$ form a complete residue system mod $(t^2 + t + 1)$. In the set of differences, the number zero appears $t + 1$ times (once for each a_i), and since there are just $t^2 + 2t + 1$ 2-permutations with repetition of the integers a_i , zero is the only number which appears more than once. Hence, the sums in pairs of the a 's are all different, for if $a_i + a_j = a_h + a_k$, then $a_i - a_k = a_h - a_j$, and further, $a_i + a_i \neq a_j + a_j$ if $i \neq j$. Therefore, if p is a prime, we have

$$(4.9) \quad F(p^2 + p + 1) \geq p + 1 .$$

Let p_m be the m -th prime. The prime number theorem is equivalent to $p_m \sim m \log m$, so that

$$(4.10) \quad \frac{p_{m+1}}{p_m} \sim 1 .$$

Now for any n , let m be the integer for which

$$p_m^2 + p_m + 1 \leq n < p_{m+1}^2 + p_{m+1} + 1 .$$

Then

$$\frac{F(p_m^2 + p_m + 1)}{\sqrt{p_{m+1}^2 + p_{m+1} + 1}} < \frac{F(n)}{\sqrt{n}} < \frac{F(p_{m+1}^2 + p_{m+1} + 1)}{\sqrt{p_m^2 + p_m + 1}} .$$

Because of (4.10) ,

$$\begin{aligned} \lim_{m \rightarrow \infty} \inf \frac{F(p_m^2 + p_m + 1)}{\sqrt{p_{m+1}^2 + p_{m+1} + 1}} &= \lim_{m \rightarrow \infty} \inf \frac{F(p_m^2 + p_m + 1)}{\sqrt{p_m^2 + p_m + 1}} \\ &= \lim_{m \rightarrow \infty} \inf \frac{F(p_{m+1}^2 + p_{m+1} + 1)}{\sqrt{p_m^2 + p_m + 1}} , \end{aligned}$$

so that

$$\lim_{n \rightarrow \infty} \inf \frac{F(n)}{\sqrt{n}} = \lim_{m \rightarrow \infty} \inf \frac{F(p_m^2 + p_m + 1)}{\sqrt{p_m^2 + p_m + 1}}$$

$$(4.11) \quad \geq 1 \quad (\text{by (4.9)}) .$$

We must now prove

$$(4.12) \quad \lim_{n \rightarrow \infty} \sup \frac{F(n)}{\sqrt{n}} \leq 1 ,$$

and then (4.8) will follow. Let $a_1 < a_2 < \dots < a_x \leq n$ be positive integers such that the sums $a_i + a_j$ ($i \leq j$) are all different, and let m be a positive integer less than n .

Consider the half-open intervals $[-m+u, u)$,

$u = 1, 2, \dots, m+n$. Let A_u denote the number of a 's in the interval $-m+u \leq a_i < u$. Each a_i occurs in m intervals, and hence

$$\sum_{u=1}^{m+n} A_u = m \times .$$

The number of pairs a_i, a_j ($i < j$) which lie in $[-m+u, u)$ is

$$\frac{1}{2} A_u (A_u - 1) .$$

Hence, if the sum over all intervals of the numbers of such pairs per interval is T , then

$$2T = \sum_{u=1}^{m+n} A_u (A_u - 1) = \sum_{u=1}^{m+n} A_u^2 - (m+n) \bar{A} ,$$

where $\bar{A} = \frac{m \times}{m+n}$. From the relation

$$0 \leq \sum_{u=1}^{m+n} (A_u - \bar{A})^2 = \sum_{u=1}^{m+n} A_u^2 - (m+n) \bar{A}^2 ,$$

it follows that

$$(4.13) \quad 2T \geq (m+n) \bar{A}^2 - (m+n) \bar{A} = m \times \left(\frac{m \times}{m+n} - 1 \right) .$$

For any pair a_i, a_j ($i < j$) lying in an interval, $a_j - a_i = r$, where $1 \leq r \leq m-1$. To each integer r in $[1, m-1]$ there corresponds at most one such pair, since the differences $a_j - a_i$ are all distinct. The pair corresponding to r occurs in exactly $m-r$ intervals, and hence

$$(4.14) \quad T \leq \sum_{r=1}^{m-1} (m-r) = \frac{1}{2} m (m-1) .$$

From (4.13) and (4.14) we obtain

$$m x(m x - m - n) \leq m (m-1)(m+n) ,$$

whence $x(m x - 2n) < m (m+n)$, and

$$m x^2 - 2 n x - m (m+n) < 0 .$$

Therefore

$$x < \frac{n}{m} + \left(\frac{n^2}{m^2} + m + n \right)^{\frac{1}{2}} .$$

We choose $m = \left[n^{\frac{3}{4}} \right]$, so that

$$x < n^{\frac{1}{2}} + O(n^{\frac{1}{4}}) .$$

Therefore $F(n) < n^{\frac{1}{2}} + O(n^{\frac{1}{4}})$, and (4.12) follows. The error term here, $O(n^{\frac{1}{4}})$, has not been improved.

Erdős, in a written communication to Stöhr, showed that for every B_2 sequence A , $\liminf_{n \rightarrow \infty} \frac{A(n)}{\sqrt{n}} = 0$, which seems surprising in view of (4.8). In the same communication he showed that on the other hand there exist B_2 sequences with $\limsup_{n \rightarrow \infty} \frac{A(n)}{\sqrt{n}} > 0$. The proofs of these two statements appear in a paper of Stöhr [31] .

The notion of B_2 sequences has been generalized by Bose and Chowla [1] . They define a B_r set as a set of non-negative integers $d_1 < d_2 < \dots$ such that the sums $d_{i_1} + d_{i_2} + \dots + d_{i_r}$ ($i_1 \leq i_2 \leq \dots \leq i_r$) are all different.

Let $F_r(x)$ be the maximum number of elements not exceeding x that a B_r set can have. Bose and Chowla prove that if m is a power of a prime and r is a positive integer, then

$$F_r(m^r) \geq m + 1 \quad (\text{cf. (4.9), where } p \text{ may be replaced by a prime power}); \text{ also } F_r(1 + q) \geq m + 2, \text{ where } q = \frac{m^{r+1} - 1}{m - 1}.$$

They prove that $\lim_{n \rightarrow \infty} \inf \frac{F_r(n)}{\frac{1}{n^r}} \geq 1$, a generalization of

(4.11), but can only conjecture the generalization of (4.12),

$$\text{namely } \lim_{n \rightarrow \infty} \sup \frac{F_r(n)}{\frac{1}{n^r}} \leq 1.$$

BIBLIOGRAPHY

- [1] Bose, R. C. and Chowla, S. "Theorems in the additive theory of numbers", American Mathematical Society Notices 7 (1960), 344.

- [2] Brauer, A. "A problem of additive number theory and its application in electrical engineering", Journal of the Elisha Mitchell Scientific Society 61 (1945), 55 - 66.

- [3] Cassels, J. W. S. "Über Basen der natürlichen Zahlenreihe", Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 21 (1957), 247 - 257.

- [4] Chatrovsky, L. "Sur les bases minimales de la suite des nombres naturels", Bull. Acad. Sci. URSS., Sér. Math. 4 (1940), 335 - 340.

- [5] Chowla, S. "Solution of a problem of Erdős and Turán in additive number theory", Proc. Nat. Acad. Sci. India, Sect A 14 (1944), 1,2.

- [6] Dirac, G. A. "Note on a problem in additive number theory", Journal London Math. Soc. 26 (1951), 312 - 313.

- [7] Erdős, P. "On a problem of Sidon in additive number theory", Acta Sci. Math. (Szeged) 15 (1954), 255 - 259.

- [8] _____ "On a problem of Sidon in additive number theory and on some related problems. Addendum", Journal London Math. Soc. 19 (1944), 208.
- [9] _____ "Problems and results in additive number theory", Colloque sur la théorie des nombres (1955), 127 - 137.
- [10] _____ "Problems in additive number theory", Report of the institute in the theory of numbers, U. of Colo., Boulder, Colo. (1959), 67.
- [11] _____ "Some results on additive number theory", Proc. Amer. Math. Soc. 5 (1954), 847 - 853.
- [12] _____ and Fuchs, W. H. J. "On a problem of additive number theory", Journal London Math. Soc. 31 (1956), 67 - 73.
- [13] _____ and Gál, I. S. "On the representation of $1, 2, \dots, N$ by differences", Proc. Acad. Wet., Amsterdam 51 (1948), 1155 - 1158.
- [14] _____ and Turán, P. "On a problem of Sidon in additive number theory, and on some related problems", Journal London Math. Soc. 16 (1941), 212 - 215.
- [15] Hardy, G. H. and Wright, E. M. "An introduction to the theory of numbers", third edition. Oxford 1954.

- [16] Hilbert, D. "Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n -ter Potenzen (Waringsches Problem)", Nachr. Ges. Wiss. Göttingen, Math-phys. Kl. (1909), 17 - 36.
- [17] _____ "Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n -ter Potenzen (Waringsches Problem)", Math. Ann. 67 (1909), 281 - 300.
- [18] Leech, J. "On the representation of $1, 2, \dots, n$ by differences", Journal London Math. Soc. 31 (1956), 160 - 169.
- [19] _____ and Hazelgrove, B.C. "Note on restricted difference bases", Journal London Math. Soc. 32 (1957), 228 - 231.
- [20] Lorentz, G. G. "On a problem of additive number theory", Proc. Amer. Math. Soc. 5 (1954), 838 - 841.
- [21] Moser, L. "On the representation of $1, 2, \dots, n$ by sums", Acta Arithmetica 6 (1960), 11 - 13.
- [22] _____ oral communication.
- [23] _____ Proposed problem no. 24, Report of the institute in the theory of numbers, U. of Colo., Boulder, Colo. (1959), 341.
- [24] Raikov, D. "Über die Basen der natürlichen Zahlenreihe", Mat. Sbornik N.S. 2 (= 44) (1937), 595 - 597.

- [25] Rédei, L. and Rényi, A. "Über die Darstellung der Zahlen $1, 2, \dots, N$ mittels Differenzen", Mat. Sbornik N.S. 24 (= 66) (1949), 385 - 389.
- [26] Rohrbach, H. "Ein Beitrag zur additiven Zahlentheorie", Math. Zeit. 42 (1937), 1 - 30.
- [27] Sidon, S. "Ein Satz über trigonometrische Polynome und seine Anwendung in der Theorie der Fourier-Reihen", Math. Annalen 106 (1932), 539.
- [28] Singer, J. "A theorem in finite projective geometry and some applications to number theory", Trans. Amer. Math. Soc. 43 (1938), 377 - 385.
- [29] Stohr, A. "Anzahlabschätzung einer bekannten Basis h -ter Ordnung", Math. Zeit. 47 (1942), 778 - 787; 48 (1942/43), 792.
- [30] _____ "Eine Basis h -ter Ordnung für die Menge aller natürlichen Zahlen", Math. Zeit. 42 (1937), 739 - 743.
- [31] _____ "Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe ", I, II. Journal reine angew. Math. 194 (1955), 40 - 65, 111 - 140.
- [32] Waring, E. "Meditationes algebraicae", Cambridge 1770, pp. 204 - 205.

B29792